From: [redacted]
[redacted]
Date: Wednesday, July 19, 2023 4:33:07 PM
Attachments: sp800-171r3-ipd-comments Planet Tech.xlsx

From: Michael Lanham [redacted]
Sent: Tuesday, July 18, 2023 9:08 PM
To: Brewer, Jeffrey (Fed) [redacted]
Subject: RE: Aw shoot for submitting comments

Jeff,

Attached, please find the considered comments from Planet Technologies. I sincerely appreciate your willingness to accommodate my admitted aw-shoot.

Very Sincerely,
Mike

Michael Lanham, Ph.D., CISSP, RPA, GPEN, …
Director of Security and Compliance, SLED & Commercial
[redacted] **Planet Technologies | https://www.Go-Planet.com**

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Dr. Lanham, Planet Technologies, Inc.	General	Publication	15	532	Add sub-paragraph c to integrate the requirement to do training with a consequence for not doing or not 'passing' training. As written, the requirement only implies the need for a consequence if users do not 'pass' training. Make the requirement to pass explicit. Planet acknowledges that this explicit tie is not within 800-53 AT-2	c. Integrate the initial and recurring training above with system access decisions (e.g., degraded or denied access as a consequence of not 'passing' the training)
2	Dr. Lanham, Planet Technologies, Inc.	General	Publication	16	559	Add sub-paragraph c to integrate the requirement to do training with a consequence for not doing or not 'passing' training. As written, the requirement only implies the need for a consequence if users do not 'pass' training. Make the requirement to pass explicit. Planet acknowledges that this explict tie is not within 800-53 AT-3	c. Integrate the role-based training above with system access decisions (e.g., degraded or denied access as a consequence of not 'passing' the training)
3	Dr. Lanham, Planet Technologies, Inc.	General	Publication	16	580	Add sub-paragraph c to integrate the requirement to do training with a consequence for not doing or not 'passing' training. As written, the requirement only implies the need for a consequence if users do not 'pass' training. Make the requirement to pass explicit. Planet acknowledges that this explict tie is not within 800-53 AT-2()2) or AT-2(3)	c. Integrate the advanced literacy training above with system access decisions (e.g., degraded or denied access as a consequence of not 'passing' the training)
4	Dr. Lanham, Planet Technologies, Inc.	General	Publication	27	998	The explicit definition of system user as 'employees or inviduals who have equivalent status to employees.' is problematic. As written, it leaves room for interpretaton that guest users, temporary users, and other forms of interactive users can be omitted from the requirement to have unique identifiers. Don't redefine terms already defined in the NIST Cyber GLossary	System users (e.g., A person or entity with authorized access) include any type (e.g., privileged usersm non-privileged users, guest users as applicable, temporary users as applicable, contractors/vendors as applicable) of person or entity and includes non-person entities (e.g., system accounts, service principal accounts, application accounts).

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
5	Dr. Lanham, Planet Technologies, Inc.	Technical	Publication	28	1026	In the vast majority of emergency "break glass" accounts I have seen, they are deliberately exempted from MFA and most other controls as they are controlled via other mechanisms. Without an explicit carve-out for known and common practice exceptions, this control causes all oranizations to 'fail' the control.	Implement multi-factor authentication for interactive access to system accounts--excluding documented and tracked emergency accounts where applicable and where MFA is not technologically supported
6	Dr. Lanham, Planet Technologies, Inc.	Editorial	Publication	31	1152	Nudge organizations toward IR plans that include not only the roadmap analogy listed, but also toward appendices that address specific scenarios--aka 'play books'. In fact, 3.6.2 specifically says 3.6.1 is supposed to generate 'types of incidents' appropriate for monitoring	a. Develop an incident response plan that provides the organization with a roadmap for implementing its incident response capability. Incorporate appendices, attachments or other supporting material to address scenarios and responses relevant to the organization (e.g., 'play books')
7	Dr. Lanham, Planet Technologies, Inc.	Technical	Publication	51	1916	Retain the explicit requirement to use FIPS validated cryptography when protecting CUI. Without the explicit requirement, it allows readers to delude themselves into thinking FIPS is no longer required when protecting CUI. The proposed change also aligns with the discussion in 3.13.8 that explicitly discusses NSA-approved Crypto	Employ FIPS-validated or NSA-approved cryptography when used to protect the confidentiality of CUI.
8	Dr. Lanham, Planet Technologies, Inc.	General	Publication	54	2060	Add para c to implement the applicable remediations or mitigations associated with the alerts, advisories, and directives. Without making a 'take action' explicit, organziations can satisfy this control without doing anything other than generating alerts, advisories, and directives	c. Implement the applicable remediations or mitigations associated with the alerts, advisories, and directives above. Track remediations or mitigations not implemented along with the risk acceptance by the appropriate authority.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
9	Dr. Lanham, Planet Technologies, Inc.	General	Publication	53	1994	as written (and as SC-7(3) is also written), there is significant ambiguity about whether an organization is penalized when it CANNOT limit external connections because one or more of its systems/sub-systems are, by design, open to public internet access (e.g., Cloud Service Offerings)	Limit the number of external network connections to the system where technically and operationally feasible. Organizations using Cloud Service Offerings (CSO) shall, to the degree feasible, limit the accessibility and functionality of the component (e.g., tenant) of their CSOs to the organization's known networks, known devices, and known users.
10	Dr. Lanham, Planet Technologies, Inc.	Technical	Publication	52	1973	As written, it is ambiguous about whether all ports and protocols must flow through a proxy. Some such protocols would fundamentally cease to function if future auditors insert 'all' into the requirement. Absent the word 'all', organizations are free to interpret this requirement. Remove ambiguity	Route internal network communications traffic to external networks through a security stack/service appropriate to the communications protocols in use where technologically feasible (e.g., web proxies, SOCKS procies) and as depicted in the security and privacy architecture.
11	Dr. Lanham, Planet Technologies, Inc.	General	Publication	57	2169	insert para c to explicitly tie violation of rules of behavior to company policy(ies) about such violations. As written, the 'consequence' for violation is only implicit. Consequences cannot be specified in a standard, but the requirement can have organizations discuss violations in their policies/procedures	c. Integrate policy, processes and/or procedures for assertions of and actual violations of the rules of behavior.
12	Dr. Lanham, Planet Technologies, Inc.	Technical	Publication	29	1077	As written, 3.5.7.e would disallow us of personal password managers (e.g., KeyPass, LastPass, 1Password) as well as key vaults such as Azure Key Vault. The language derives from IA-5's discussion about system-stored passwords.	e. Systems will store passwords only in appropriately protected password vaults, containers, or services when it is necessary to retain the entirety of clear-text passwords. Organizations shall track the storage location(s) and use(s) of such system-stored clear-text passwords.
13	Dr. Lanham, Planet Technologies, Inc.	General	Publication	35	1313	The discussion unnecessarily limits itself to system media, when the requirement explicity addresses digital and non-digital media	Access to CUI on digital and nondigital ~~system~~ media can be restricted….

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
14	Dr. Lanham, Planet Technologies, Inc.	General	Publication	35	1329	The sentence that starts, "Organizations determine the appropriate.." seems contradictory to the next sentence that says "NARA policies control the sanitization process for CUI." Remove the ambiguity and require organizations follow NARA policies.	~~Organizations determine the appropriate sanitization methods with the recognition that destruction is sometimes necessary when other methods cannot be applied to media that require sanitization.~~ NARA policies control the sanitization process for CUI and may require destruction when other methods cannot be applied to media .
15	Dr. Lanham, Planet Technologies, Inc.	Editorial	Publication	36	1337	As written, there is no room for use of the Standard Form (SF) SF-902 CUI Purple label nor the use of the SF-901 CUI Cover Sheet. Also as written it only addresses 'system media' and not digital and non-digital media, which the base requirement emphasizes	a. Mark digital and non-digital media in accordance with NARA publications. Where feasible and appropriate, organizations should use US Government (USG) Standard Form (SF) 902 and SF 903 Media Labels (CUI) to mark devices/media that store, process, or transmit CUI (e.g., such labels imbalance spinning optical media, do not use them on such media). Where feasible, organizations should use USG SF-901 CUI Coversheet to protect the confidentiality of non-digital media (e.g., papers, binders, folders).
16	Dr. Lanham, Planet Technologies, Inc.	General	Publication	38	1422	Insert a new paragraph explicitly addressing the constant refrain about access to CUI by non-US Citizens/non-US persons. Since the creation authority for CUI starts at the Federal level, there should be guidance telling organizations to seek clarity from the Government entity(ies) that created the CUI about whether non-US persons may access the CUI. The replies to public comments in CFR effectively said what I am proposing since there is too much variability for any single guidance document to capture it all and the CFR demurred from explicitly giving an answer while directing readers to their CUI-granting government entity.	Determining whether non-US citizens should, or should not, have access to particular CUI is beyond the scope of this standard. Organizations seeking to share non-export controlled CUI with non-US citizens should seek clarifying guidance from the CUI-originating government entity(ies). Export Controls have their own regulatory frameworks (e.g., ITAR, EAR) which this document does not repeat. Organizations seeking to have non-US Citizens as privileged users or maintenance personnel of CUI-processing devices should seek clarifying guidance as well. Organizations should be prepared to segment CUI access based on different guidance from those CUI-originating government entities.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
17	Dr. Lanham, Planet Technologies, Inc.	General	Publication	44	1648	Insert a new sentence to describe how an organization communicates to itself and others risk acceptance decisions, especially since the discussion just finished mentioning the possiblity of 'accept risk' as a response to findings	...needed. Should organizations choose to accept risks, they must keep track of the accepted risks (e.g., multi-purposing their POAM to indicate a status of risk accepted) and add review of existing risk acceptances to their periodic review requirements (see also 3.12.3). However,...
18	Dr. Lanham, Planet Technologies, Inc.	Editorial	Publication	45	1682	Be explicit there there is no defined requirement AND point readers to the NIST 800-171 home page	Develop a plan of action and milestones for the system to support risk-based decisions by organizational leadership. There is no defined format for a POAM, though NIST does make one available on the SP 800-171.
19	Dr. Lanham, Planet Technologies, Inc.	Editorial	Publication	45	1686	add a 3rd numbered paragraph for 3.12.2.a to remove ambiguity about whether items in a POAM get deleted or not (they should not...it is part of an evidentiary trail)	3. To provide a longitudinal record of weaknesses or deficiencies, remediations, mitigations, risks accepted (as applicable), and support measures of effectiveness for such efforts.
20	Dr. Lanham, Planet Technologies, Inc.	Editorial	Publication	45	1686	add a 3rd paragraph for 3.12.2	c. Incorporate the POAM and its review into the organization's risk assessment(s) policy, processes, and procedures supporting organizational leadership's risk-based decisions.
21	Dr. Lanham, Planet Technologies, Inc.	General	Publication	47	1774	As written (and taken from SC-7) the c paragraph (3.13.1.c) can and sometimes is interpreted as not authorizing access to 3rd party cloud service providers except through company provided security stacks. Creative interpretations argue that company provided VPN on endpoints is a managed interface so access from telework locations is covered via VPN. Change this to allow the boundary protection to allow capabilities in those external systems to provide 'boundary' protect for the organizations' tenant within those CSO	c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. The boundary devices may be on-premises, or may be part of the external services (e.g., protection capabilities built into cloud service offerings (CSO) that provide the organization insight and control of connections to/from its CSO, or may be in some other configuration that secures the logical boundary(ies) of the organization.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
22	Dr. Lanham, Planet Technologies, Inc.	General	Publication	49	1835	Restore the ODP offered in the SC-7(5) that allows organizations to do the control at managed interface and/or for organization-defined systems. This allows organizations to implement inbound DAPE at security boundaries and have deliberately more open policies for outbound traffic--especially where it is infeasible to capture all forms of outbound traffic (e.g., colleges involved in research supporting DoD)	Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]]
23	Dr. Lanham, Planet Technologies, Inc.	Editorial	Publication	21	768	Though the language is straight out of CM-2, I propose to modify the first sentence to incorporate language from the description that deliberately pluralizes the word system and emphasizes 'baseline' can also apply to components of the system	a. Develop, document, and maintain under configuration control, a current baseline configuration(s) of the system(s) and/or system components. b. Review and update the baseline configuration(s) of the system and/or system components [Assignment: organization-defined frequency] and when system(s) and/or system components are installed or upgraded.
24							767
25							
26							