From: **Todd Thiemann** <<u>todd@privatecore.com</u>> Date: Fri, Nov 8, 2013 at 7:31 PM Subject: Preliminary Cybersecurity Framework Comments To: <u>csfcomments@nist.gov</u>

Dear Sir/Madam,

I am writing regarding the NIST preliminary Cybersecurity Framework was published in October

(http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf) with a suggestion to improve the document. I understand from the webpage <a href="http://www.nist.gov/itl/cyberframework.cfm">http://www.nist.gov/itl/cyberframework.pdf</a>) with a suggestion to improve the document. I understand from the webpage <a href="http://www.nist.gov/itl/cyberframework.cfm">http://www.nist.gov/itl/cyberframework.pdf</a>) with a suggestion to improve the document. I understand from the webpage <a href="http://www.nist.gov/itl/cyberframework.cfm">http://www.nist.gov/itl/cyberframework.cfm</a> that this is the right email address for comments. I have attached the spreadsheet template with my propose change.

The document includes provisions to secure data at rest ("PR.DS-1: Protect data (including physical records) during storage (aka "data at rest") to achieve confidentiality, integrity, and availability goals") and in motion ("PR.DS-2: Protect data (including physical records) during transportation/ transmission (aka "data in motion") to achieve confidentiality, integrity, and availability goals"), but includes no mention of "data in use". When one considers the lifecycle of data (at rest, in motion/transit, in use), this oversight leaves a "data in use" hole in the cybersecurity framework.

Note that other NIST publications make reference to data in use alongside data in motion and data at rest. NIST Special Publication 500-299, "NISTCloud Computing Security Reference Architecture" page 107 under "Cryptographic Services" makes reference to data-in-use (available at <a href="http://collaborate.nist.gov/twiki-cloud-computing/pub/">http://collaborate.nist.gov/twiki-cloud-computing/pub/</a>

 $CloudComputing/CloudSecurity/NIST\_Security\_Reference\_Architecture\_2013.05.15\_v1.0.pdf\ .$ 

The Cloud Security Alliance framework includes data-at-rest, data-in-motion, and data-in-use (refer to <a href="https://research.cloudsecurityalliance.org/tci/index.php/explore/security\_risk\_management/">https://research.cloudsecurityalliance.org/tci/index.php/explore/security\_risk\_management/</a> ).

My proposal is to include mention of data in use in the document. What I propose is a section alongside PR.DS-1 and PR.DS-2 that would have the following:

\_\_\_\_

Protect data (including physical records) during use (aka "data in use") to achieve confidentiality, integrity, and availability goals.

\_\_\_\_

I believe this change would supported by COBIT APO01.06, BAI02.01, BAI06.01, DSS06.06 and ISO/IEC 27001 A.15.1.3, A.15.1.4.

Please let me know the process for integrating this sort of feedback into the document and if I can elaborate on this suggestion.

Best regards,

Todd

See Attached.

Γ	<b># O</b>	rganizati	Comment	Тур	Pag	Lin	Section	Comment (Include rationale for	Suggested change
	on	n	or	e	e #	e #		comment)	
	on	U					Section Appendi x A, Table 1	comment)The framework includes data at rest("PR.DS-1: Protect data (includingphysical records) during storage (aka"data at rest") to achieve confidentiality,integrity, and availability goals") and inmotion ("PR.DS-2: Protect data (includingphysical records) during transportation/transmission (aka "data in motion") toachieve confidentiality, integrity, andavailability goals"), but includes nomention of "data in use". When oneconsiders the lifecycle of data (at rest, inmotion/transit, in use), this oversightleaves a "data in use" hole in thecybersecurity framework.Note that other NIST publications makereference to data in use alongside data inmotion and data at rest. NIST SpecialPublication 500-299, "NIST CloudComputing Security ReferenceArchitecture" page 107 under"Cryptographic Services" makes referenceto data-in-use (available athttp://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.1	The framework includes data at rest ("PR.DS-1: Protect data (including physical records) during storage (aka "data at rest") to achieve confidentiality, integrity, and availability goals") and in motion ("PR.DS-2: Protect data (including physical records) during transportation/ transmission (aka "data in motion") to achieve confidentiality, integrity, and availability goals"), but includes no mention of "data in use". When one considers the lifecycle of data (at rest, in motion/transit, in use), this oversight leaves a "data in use" hole in the cybersecurity framework. Note that other NIST publications make reference to data in use alongside data in motion and data at rest. NIST Special Publication 500-299, "NIST Cloud Computing
								1 0	-

onoree#comment)makes reference to data-in-use (available at http://collaborate.nist.gov/twi kdata-at-rest, data-in-motion, and data-in-use (refer to https://research.cloudsecurityalliance.org/t ci/index.php/explore/security_risk_manag ement/ ).makes reference to data-in-use (available at http://collaborate.nist.gov/twi kdi-cloud-computing/pub/My proposal is to include mention of data in use in the document. What I propose is a section alongside PR.DS-1 and PR.DS-2 that would have the following:Protect data (including physical records) during use (aka "data in use") to achieve to offidentiality, integrity, and availability goalsThe Cloud Security Alliance framework includes data-at-rest, data-in-motion, and data-in-use (refer to https://research.cloudsecuritya lliance.org/tci/index.php/exploNy proposal is to include mention of data in use") to achieve to achieve to fully confidentiality, integrity, and availability goals.The Cloud Security Alliance framework includes data-at-rest, data-in-motion, and data-in-use (refer to https://research.cloudsecuritya lliance.org/tci/index.php/exploNy proposal is to include mention of data in use in theNy proposal is to include mention of data in use in the	on         or         e         e #         comment)         makes reference to data-in- (available at https://research.cloudsecurityalliance.org/ti ci/index.php/explore/security_risk_manag ement/ ).         makes reference to data-in- (available at http://collaborate.nist.gov/ ki-cloud-computing/pub/ ki-cloud-computing/CloudSec ty/NIST_Security_Referen My proposal is to include mention of data in use in the document. What I propose is a section alongside PR.DS-1 and PR.DS-2 that would have the following: ====         The Cloud Security Alliance framework includes data-at- rest, data-in-motion, and data-in- use (refer to https://research.cloudsecurity.alliance.org/ti in use in the document. What I propose is a section alongside PR.DS-1 and PR.DS-2 that would have the following: =====         The Cloud Security Alliance framework includes data-at- rest, data-in-motion, and data- in-use (refer to https://research.cloudsecurity goals. ===== This would be supported by · COBIT APO01.06, BAI02.01, BAI06.01, DSS06.06 and ISO/IEC 27001 A.15.1.3, A.15.1.4.         My proposal is to include mention of data in use in the motion of data in use	Organizati	Suggested change	n Section Comment (Include rationale for	Section	Lin	Pag	Тур	Comment	Organizati	#
data-in-use (refer to https://research.cloudsecurityalliance.org/t ci/index.php/explore/security_risk_manag ement/).(available at http://collaborate.nist.gov/twi ki-cloud-computing/pub/ CloudComputing/Dub/ CloudComputing/Dub/ CloudSecurity_Reference_ Architecture_2013.05.15_v1.0 .pdf .My proposal is to include mention of data in use in the document. What I propose is a section alongside PR.DS-1 and PR.DS-2 that would have the following: ==== Protect data (including physical records) during use (aka "data in use") to achieve confidentiality, integrity, and availability goals. ==== This would be supported by · COBIT APO01.06, BA102.01, BA106.01, DSS06.06 and ISO/IEC 27001 A.15.1.3, A.15.1.4.The Cloud Security Alliance framework includes data-at- rest, data-in-motion, and data- in-use (refer to https://research.cloudsecuritya lliance.org/tci/index.php/explo re/security_risk_management/ ).	data-in-use (refer to https://research.cloudsecurityalliance.org/t ci/index.php/explore/security_risk_manag ement/ ).(available at http://collaborate.nist.gov/t ki-cloud-computing/pub/ CloudComputing/CloudSec ty/NIST_Security_Referen Architecture_2013.05.15_v .pdf .My proposal is to include mention of data in use in the document. What I propose is a section alongside PR.DS-1 and PR.DS-2 that would have the following: ====The Cloud Security Alliand framework includes data-at rest, data-in-motion, and da in-use (refer to https://research.cloudsecuri goals. ==== This would be supported by · COBIT APO01.06, BAI02.01, BAI06.01, DSS06.06 and ISO/IEC 27001 ).The Cloud security and availability resecurity_risk_management o.My proposal is to include mention of data in use in the during use (aka "data in use") to achieve to offidentiality, integrity, and availability goals. ==== This would be supported by · COBIT APO01.06, BAI02.01, BAI06.01, DSS06.06 and ISO/IEC 27001 ).My proposal is to include mention of data in use in the mention of data in use in the			comment)		e #	e #	e	or		
a section alongside PR.DS-1 and PR.DS-2 that would have the following: ==== Protect data (including physical records) during use (aka "data in use") to achieve	a section alongside PR.DS- and PR.DS-2 that would ha the following: ==== Protect data (including physical records) during us (aka "data in use") to achie		<ul> <li>(available at http://collaborate.nist.gov/twi ki-cloud-computing/pub/ CloudComputing/CloudSecuri ty/NIST_Security_Reference_ Architecture_2013.05.15_v1.0 .pdf .</li> <li>The Cloud Security Alliance framework includes data-at- rest, data-in-motion, and data- in-use (refer to https://research.cloudsecuritya lliance.org/tci/index.php/explo re/security_risk_management/ ).</li> <li>My proposal is to include mention of data in use in the document. What I propose is a section alongside PR.DS-1 and PR.DS-2 that would have the following: ===== Protect data (including physical records) during use</li> </ul>	<ul> <li>includes data-at-rest, data-in-motion, and data-in-use (refer to https://research.cloudsecurityalliance.org.ci/index.php/explore/security_risk_management/).</li> <li>My proposal is to include mention of data in use in the document. What I propose i a section alongside PR.DS-1 and PR.DS-that would have the following:</li> <li>====</li> <li>Protect data (including physical records) during use (aka "data in use") to achieve confidentiality, integrity, and availability goals. ==== This would be supported by · COBIT APO01.06, BAI02.01, BAI06.01, DSS06.06 and ISO/IEC 2700</li> </ul>		e #	e #	e	or		