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

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 http://www.nist.gov/itl/cyberframework.cfm 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 http://collaborate.nist.gov/twiki-cloud-computing/pub/

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 https://research.cloudsecurityalliance.org/tci/index.php/explore/security_risk_management/).

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.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	PrivateCore	Todd Thiemann	G	18	466	Appendix A, Table 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 Security Reference Architecture” page 107 under "Cryptographic Services" makes reference to data-in-use (available at http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf . The Cloud Security Alliance framework	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 Security Reference Architecture” page 107 under "Cryptographic Services"

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
							includes data-at-rest, data-in-motion, and data-in-use (refer to https://research.cloudsecurityalliance.org/tci/index.php/explore/security_risk_management/). 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, BAI02.01, BAI06.01, DSS06.06 and ISO/IEC 27001 A.15.1.3, A.15.1.4.	makes reference to data-in-use (available at http://collaborate.nist.gov/twiki-cloud-computing/pub/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 https://research.cloudsecurityalliance.org/tci/index.php/explore/security_risk_management/). 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.