NCDPI Response

From: Rob Dietrich
Sent: Tuesday, July 11, 2023 11:20 PM
To: Sara Kloek

Good Evening,

Thank you for your questions regarding third-party data integration. Please see the questions and answers below:

- Question: Will vendors be required to comply with laws and regulations that do not apply to them (FOIA, NARA, etc.)?
    - Answer: You must comply with any applicable state and federal laws.

- Question: Will all ed tech companies need to comply with the standards or just those that integrate with a learning management system or other school system?
    - Answer: Any company that receives student data from a state system will have to follow this process.

- Question: How will the vendor security and system architecture information be protected by DPI to avoid the risk of these roadmaps getting accessed by bad actors?
    - Answer: This information would be delivered to the PSU and not to DPI. Therefore, we would not receive any information.

- Question: Will there be any efforts to streamline this reporting so each vendor does not need to do the same thing for each PSU?
    - Answer: This process is to be done by PSUs using the service.

- Question: Does the DPI Frequently Asked Questions: Third Party Vendor Data Integration, #4, mean that new or renewal contracts signed before August 1, 2023 (even if the contract goes into effect on or after August 1, 2023) are not impacted by the new DPI process?
    - Answer: As long as it is fully executed by August 1, 2023, this is correct.

- Question: We kindly note that it would be operationally difficult, if not impossible, for software vendors to comply with certain Service Agreement provisions as written (e.g., vendor to request PSU's advance written approval of

subcontractor and purpose of disclosure prior to sharing Shared Data with any subcontractors). Will DPI and/or PSUs be permitted to negotiate the Service Agreement?
    - Answer: There are to be no changes to the Data Security Agreement.

- Question: May a vendor provide either a VRAR or a third-party conducted assessment report?
    - Answer: No. You must complete both. The VRAR is only done once upon initial contract and the third party conducted assessment must be completed initially and then annually.

- Question: FIPS 140-2/-3 is referenced in the "Vendor Readiness Assessment Report (VRAR) for Solutions Not Hosted on State Infrastructure" document. Is FIPS 140-2/-3 certification a requirement or is it acceptable for cryptography practices that are aligned with FIPS 140-2/-3 sufficient?
    - Answer: Certification is not a requirement, cryptography practices that align with FIPS140-2/3 and NIST 800-53 are acceptable.

Rob

Rob Dietrich, Ed.D., CeCTO, IPT, CETL
Senior Director
Office of Digital Teaching and Learning
Division of Digital Learning and Technology Services