Questions and Answer from Session 1. An Overview of the Tips and Tools

Question: *What is the website where the cybersecurity information is shared?*

Answer: https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

Question: *Is the security framework plan being discussed a TEA mandate?*

Answer: No. The security framework plan and the tips and tools are recommendations to address cybersecurity issues being encountered by the education community and improve overall cybersecurity posture.

Question: *Are the cybersecurity webinars being recorded and will they be available for future review?*

Answer: Yes. The cybersecurity webinars are being recorded and will be available to view at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools.

Question: *You mentioned some available courses. How can I access them?*

Answer: *The free online training discussed in the webinar regarding cyber security and IT related topics is available through an online resource called Cybrary. More information regarding Cybrary is available at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools.*

Questions and Answers from Session 4. Incident Response, Being Prepared

Question: Can you tell me the difference between internal FERPA versus external FERPA release?
An educational agency or institution may disclose FERPA-protected information without parental consent to other school officials, including teachers, within the agency or institution if the agency or institution has determined the officials have a legitimate educational interest. A contractor, consultant, volunteer, or other party to whom the school district has outsourced institutional services or functions may be considered a school official provided the party performs a function for which the district would otherwise use employees and is under the direct control of the district in regard to the use and maintenance of education records. Neither FERPA nor its regulations define the required legitimate educational interest a school official must have to justify disclosure internally, but DOE has stated a school official generally has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility. The FERPA regulations provide if an educational agency or institution wishes to disclose education records without parental consent under the "school officials" exception, it must establish policies delineating which employees qualify as school officials and what constitutes a legitimate education interest.

Question: Many Student Information Systems (SIS) have a place for shot records, medicine taken by a student, etc. If a SIS is used by a nurse to track this information is that data

subject to HIPAA rules and in turn do the districts have to follow HIPAA rules?
Student health records, including immunization records, maintained by an educational agency or institution, including records maintained by a school nurse, are education records subject to FERPA. HIPAA's regulations state that records that are subject to FERPA are not subject to HIPAA.

Question: How does HIPAA relate to this and to the district? Does it impact a breach in some way differently?
HIPAA's regulations state that records that are subject to FERPA are not subject to HIPAA. Student health records, including immunization records, maintained by an educational agency or institution, including records maintained by a school nurse, are education records subject to FERPA.

Question: May I get a copy of the Incident Response Team Red Book?
Yes, the Incident Response Team Red Book is available for download by clicking on the hyperlink, and it is also located at the bottom of the page under Related Items, documents.

Question: Will a copy of the PowerPoint presentation be made available for the attendees?
Yes, the slide deck is posted at: https://www.texasgateway.org/ in the Cybersecurity Tips and Tool section along with a recording of the presentation, Incident Response: Being Prepared, Session 4.

Question: Is there any additional coordination we need to do with our Education Service Centers?
Anytime you are dealing with a potential exposure of sensitive identifying information, I recommend coordinating with your ESC. They can be a valuable resource and also alert other ESCs of a potential threat which might prevent additional similar exposures. Please do not hesitate to contact Frosty Walker at frosty.walker@tea.texas.gov or 512 463-5095 for assistance.

Question: When will TEA stop requiring SSNs (except for the one time generating of TSDS numbers and then using TSDS number thereafter)?
TEA works with other entities such as institutes of higher education and the Texas Work Commission which need the SSN to correlate information as students progress into higher education and into the workforce.

Question: What is the best process to use when data is published to the web and is accessible through Google and while you can remove the source document, Google keeps the document available on the cache?
You can notify Google but it will take days before its gone. Should you experience an exposure of sensitive information at a website which you do not control, you will need to work with the site ownership to remove the data. This may take time and the data may continue to be cached for several days. This is a situation in which law enforcement may be able to assist.

Question: In a decentralized environment, which department should champion if not push Cybersecurity initiatives? We do not have a CISO.

In most decentralized environments, the Information Technology department; however, that decision should be made by your leadership.

Question: What is the URL for the Texas Gateway?
https://www.texasgateway.org/

Question: Will you please post the slide deck from this presentation?
Yes, the slide deck is posted at: https://www.texasgateway.org/ in the Cybersecurity Tips and Tool section along with a recording of the presentation, Incident Response: Being Prepared, Session 4.