Q&A for SDBOR IT Security Assessment Continued

144. Will the Board of Regents extend the due date two weeks from December 7 to December 21, 2023?

     The BOR will not offer a two week extension, however the date for proposal submission has been extended to December 8, 2023.

145. Do you want the assessments of the Board of Regents and the six institutions performed in parallel or sequentially?

     They do not need to be conducted all in parallel nor sequentially as timelines for best availability will likely vary between institutions. A schedule can be adapted to meet the vendor's and institutions best capacity and availability.

146. What is the start date of the project? What is the desired project end date?

     We would like to complete the assessments in the first half of 2024 and ideally would start in February or March to be consistent with previous internal assessments.

147. Cyber Insurance is stated as a compliance framework. What are the requirements of this framework? Are these requirements documented in a format that can be shared with the potential bidders?

     Cyber insurance can vary greatly, and we are currently vetting out all options as it relates to this area. This requirement is not structured to one set of requirements but rather a generalization of typical insurance requirements (MFA, immutable backups, PAM, etc..)

148. What are the expectations of the physical security assessment?

     The physical security assessment is of less importance to the system but would include a walkthrough of on-site data centers for any glaring lapses or issues as it relates to security or resiliency.

149. Are non-digital systems providing physical security considered within scope of this assessment?

     The physical security assessment is of less importance to the system but would include a walkthrough of on-site data centers for any glaring lapses or issues as it relates to security or resiliency. This could include non-digital controls or systems, but no formal review is necessary.

150. Are digital systems providing physical security considered within scope of this assessment?

The physical security assessment is of less importance to the system but would include a walkthrough of on-site data centers for any glaring lapses or issues as it relates to security or resiliency. This could include digital controls or systems, but no formal review is necessary.

151. Are Operational Technology Network(s) supporting environmental control and monitoring systems considered within scope of this assessment?

Not considered in scope.

152. If Operational Technology Network(s) supporting environmental control systems are within scope of this assessment, are these OT Networks separate from each University's academic Information Technology Networks?

Not considered in scope.

153. If Operational Technology Network(s) supporting environmental control systems are within scope of this assessment, are these OT Networks included in the number of "Active Hosts" targets listed in RFP Section 3.2.1.3.5?

Not considered in scope.

154. Is Wi-Fi security assessment in scope?

Not in scope.