Cybersecurity Assessment Tool for Transit Webinar Participant Questions

March 1, 2023
1:00 PM – 2:00 PM
Presentation | Recording | Cybersecurity Assessment Tool for Transit (CATT)

Question: Are these cyber tips suggestions or Federal Transit Administration mandates? When will they be mandatory? If so?

Answer: The tool is not mandatory or required by FTA. Transit agencies can use CATT as a best practice tool for self-assessment.

Question: Is this like the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Evaluation Tool (CSET) and Cyber Resilience Review (CRR)?

Answer: Yes, the CATT leverages the CRR as the basis for its questions and structure. The project team then streamlined the tool to make it more accessible for public transit agencies. It included transit-specific language and concepts to allow agencies to further develop their cybersecurity awareness and understanding.

Question: How does this approach differ/is similar to the National Institute of Standards and Technology (NIST) Cyber Security Framework?

Answer: The NIST Cyber Security Framework (CSF) was used as the foundation for the CATT. The report also includes mapping the NIST CSF so that agencies can understand their coverage relative to the framework.

Question: How can private transportation companies/establishments be part of this evolving safety assessment tool apparatus within the overall transit ecosystem?

Answer: Stakeholder engagement with industry partners or public transit agencies is key to addressing the needs and designing solutions that meet those demands. Your questions and comments help FTA further develop its assessment tools or advance technologies for the overall transit ecosystem. A good method would be more participation from private providers and public transit agencies in FTA webinars, like the CATT webinar, including questions and making comments.

Question: This is great, but it is a huge amount of information for our small/mid-sized agency. How do you recommend we proceed and make progress without overwhelming the IT and admin staff?

Answer: The CATT is designed precisely to address this challenge. The tool helps prioritize gaps in what you are already doing to help you move closer towards a comprehensive cybersecurity program.

Question: Can this apply to both public and private transportation service providers?

Answer: Yes, the tool applies to both public and private transportation services.

Question: Is there any kind of certification after this?

Answer: At this time, CATT does not include a certification process.

Question: Do you have suggestions on how to handle CATT in situations where IT and *Supervisory Control and Data Acquisition* (*SCADA)* networks are separate and possibly have different control and maturity levels?

Answer: CATT is focused on providing a comprehensive view of your overall cybersecurity program. The maturity of IT and SCADA networks is only one of many facets of your overall program covered by CATT.

Question: Does this tool generate an action plan for a transit agency to implement?

Answer: The tool provides a prioritized order of the domains the agency should focus on with resource guides to support the next steps.

Question: Should the assessment capture all organization's critical assets or only related to the transit operations?

Answer: We believe that the questions are comprehensive, covering the full scope of an organization's cybersecurity program.

Question: Are we able to share the information about CATT in our newsletter?

Answer: Yes. You can also include a link to the FTA website to download the tool.

Question: Do we have to submit this report to FTA periodically?

Answer: No. CATT is a self-assessment tool, not a requirement by FTA. It is not required to share the report outside of your organization.

Question: Can you explain more about the CRR and how it fits with CATT?

Answer: The CATT used the CRR as the basis for the tool. The project team identified opportunities to streamline the CRR and iterate the language for the public transit use case, resulting in the CATT.

Question: What other resources are available through CISA, NIST, and DHS?

Answer: The FTA page for cybersecurity has links to other resources.

Question: Based on past experiences, how long did the assessment take when all parties were together to answer these questions?

Answer: The process generally takes a day to a day and a half.

Question: Have you integrated this approach with the Rail Safety and Security Oversight program? It seems to me this would be useful to this program.

Answer: The CATT assessment is not a requirement, but any transit agency, bus or rail, private or public, can use it to conduct a self-assessment.

Question: I am the first IT person for an organization and trying to bring things under control. What are the top 3 areas on which I should focus my cybersecurity efforts with limited IT resources?

Answer: We suggest you leverage the CATT to understand what the organization is doing and highlight and prioritize existing vulnerabilities.

Question: Are you recommending that this assessment (tool) is used (updated) each year?

Answer: As a best practice, an organization should assess its cybersecurity program at least once per year.

Question: Are TSA and FTA collaborating to unify their efforts in assessing industry readiness and establishing best practices?

Answer: TSA and FTA coordinate in many areas of transit security, including cybersecurity but have yet to establish any joint requirements or guidelines for assessing industry readiness.

Question: How many critical services do you suggest agencies evaluate, and can you give examples of critical services?

Answer: Please review the CATT for further information on critical services.

Question: Please restate the list of recommended stakeholders to include in the assessment process/discussion.

Answer: The executive leadership team, including the CFO, head of IT, head of physical security, head of operations, and the general counsel.

Question: Will this tool be updated periodically, and can we suggest additional questions to be included should they arise?

Answer: At this point, FTA has no plans to update CATT periodically. We will assess feedback and comments about the tool and, based on the feedback and comments and make a decision about updating the CATT and the assessment questions.

Question: Who developed this tool, and how long did it take?

Answer: FTA funded this tool development project with the Rock Island County Metropolitan Mass Transit District (MetroLINK) and its partners Max Cybersecurity and Grayline Group in 2021.