Response to Written Question Submitted by Hon. John Thune to Hon. John Roth

Question. How is TSA progressing towards a risk-based strategy for non-aviation transportation systems. Your September 9th report identified TSA's deficiencies in this area and made several recommendations. I concurred with your concerns and in September introduced the Surface Transportation and Maritime Security Act which would require TSA to develop a risk-based strategy. Have you seen progress from TSA in developing a strategy that first identifies the risks and then determines the proper funding levels?

Answer. On November 21, 2016, TSA provided us with an update on the actions it has taken to address the recommendations in our report, *TSA Needs a Crosscutting Risk-Based Security Strategy* (OIG-16-134). TSA indicated that it expects to complete a risk-based security strategy that encompasses all transportation modes in the fourth quarter of FY 2017. TSA is also taking steps to integrate enterprise risk management with resource planning and expects to complete this process by December 31, 2020. We will continue to monitor TSA's progress on addressing our recommendations.

Response to Written Questions Submitted by Hon. Deb Fischer to Hon. John Roth

Question 1. Mr. Roth, you referenced the 9/11 Act and that TSA has not fulfilled several rail security directives, including identifying high risk carriers. Has the TSA indicated its intention to carry out these directives and strengthen rail security?

Answer. On November 29, 2016, TSA provided us with an update to the recommendations we made in our report, *TSA Oversight of National Passenger Rail System Security* (OIG-16-91). TSA has designated the rulemakings as high priority and indicated it is making progress. On December 16, 2016, TSA published two rulemakings in the Federal Register:

- *Notice of proposed rulemaking for Security Training for Surface Transportation Employees* and
- *Advance notice of proposed Rulemaking for Surface Transportation Vulnerability Assessments and Security Plans*.

TSA anticipates a Notice of Proposed Rulemaking for surface security vetting by the end of 2017.

Question 2. There are concerns about the GAO's recommendations for “alternative” credentialing methods, including the potential for a decentralized system (whereby each entity have their own port security systems). Can you elaborate further on these concerns?

Answer. We did not review “alternative” credentialing methods in our audit, *TWIC Background Checks are Not as Reliable as They Could Be* (OIG-16-128). However, during site visits at two ports, we observed that port workers were required to have a valid TWIC as well as airport issued credential to access certain port areas. We believe there could be increased security risks if TSA adopts “alternative” credentialing methods because the Department would have to provide oversight to ensure the decentralized credentialing methods meet minimum security requirements.

Question 3. What are your thoughts on the United States Coast Guard's (USCG) August 2016 final rule that will require high-risk category facilities and a vessel to incorporate an electronic TWIC validation process, which includes a biometric check for high-risk category facilities and a vessel, prior to entry into a secured area?

Answer. The final rule was published after we completed our audit field work. Additionally, TWIC implementation at facilities and vessels was outside the scope of our review, which focused on the TSA background check process. GAO identified in its 2011 audit that unless TSA strengthens its background check process, there is a risk that someone can access a secured area with a fraudulently obtained TWIC card whether or not the facility uses a card reader. We agree with GAO’s assessment.

Question 4. The August 2016 TWIC reader rule also states that, while not required, a maritime operator can utilize electronic TWIC inspection on a voluntary basis if they feel that this provides an additional level of security protection - and many have chosen to incorporate TWIC electronic readers into their USCG facility security plans. Are you seeing the biometric check being utilized beyond the category facilities that will be subject to USCG Final Rule?

Answer. Voluntary use of electronic card readers was outside the scope of our audit. We attempted to obtain a listing of all facilities that use electronic card readers for background informational purposes only; however, USCG officials told us they were unable to provide that information. We may pursue this topic during a future audit.