COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity, Infrastructure Protection, and Innovation Subcommittee Chairman Cedric Richmond (D-LA)

Securing U.S. Surface Transportation from Cyber Attacks

Joint Hearing – the Subcommittee on Transportation and Maritime Security and the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation

February 26, 2019

Last fall, our Subcommittees held a joint hearing to assess cybersecurity risks to aviation. We learned that cyber threats to aviation are persistent, that cyber tools can be used to engage in cyber espionage or undermine confidence in the aviation industry, and that the safety of air travelers requires us to stay a step ahead of bad actors.

In short, we learned that the cybersecurity posture of the aviation sector is a national security, economic security, and public safety imperative. The same can be said for the cybersecurity posture of our surface transportation systems.

Surface transportation includes roads, rail, maritime facilities, and pipelines, and my district is rich in all of them, so I'm glad we are beginning the 116th Congress with this hearing. Compared to the aviation sector, surface transportation receives relatively little in Federal funding to support security.

Outside of the Transit Security Grant Program – which is awarded to public transportation entities and primarily used to secure against physical threats – surface transportation owners and operators foot the bill for security themselves.

But the Federal government is not off the hook. It plays a critical role in providing the situational awareness, security assessments, and guidance to stakeholders that inform surface transportation security investments.

In the decade and a half since it was established, the Department of Homeland Security has matured its ability to convene stakeholders, leverage its cross-component expertise, and share actionable intelligence analysis and guidance to help address pressing national security challenges.

Whether or not the Federal government can effectively partner with stakeholders to secure surface transportation modes from cyber attacks rests on DHS' ability to continue to perform and build on these capabilities.

Approximately 125,000 miles of pipelines – valued at $1.9 billion - move oil and gas through Louisiana every day. The industry employs over 2,500 people in the State. Toward that end, I was pleased that the Pipeline Cybersecurity Initiative was one of the first priorities announced by the new National Risk Management Center last year and the updated Pipeline Security Guidelines were finally released last March. I am encouraged that the Department is redoubling its efforts to improve the cybersecurity of pipelines by enhancing the in-house collaboration between CISA and TSA and engaging with the private sector.

I believe the Pipeline Cybersecurity Initiative has the potential to provide a more comprehensive understanding of the unique cybersecurity risks to pipelines, particularly as the sector relies more on the industrial internet of things. That knowledge will empower stakeholders to address cybersecurity risks more strategically. Although the Initiative was first announced as one of the NRMC's initial "sprint," I hope that it will evolve into a more permanent collaboration. I am concerned, however, that the updated Pipeline Security Guidelines do not address supply chain risk management.

Moreover, I will be interested to know how TSA is implementing the 10 recommendations the Government Accountability Office made in December related to its management of the Pipeline Security Program. The safety of my community and the economy of my district depend on DHS getting this mission right.

I would be remiss if I did not also raise my concerns about the cybersecurity posture of both passenger and freight rail, particularly as passenger rail cars incorporate automatic train control, network and trainline control, and monitoring and diagnostics, among other technologies. Last month, I read troubling reports of a Chinese rail company significantly underbidding competitors to win transit rail contracts in four major markets.

I am aware of China's political and economic ambitions. The intelligence community and Congress have been clear in cautioning against the use of Chinese telecommunications products.

But it is unclear to me whether the Federal government has assessed what, if any, additional cybersecurity threat is posed by contracting with a Chinese company to purchase railcars with advanced technologies.

It is also unclear whether the Federal government is providing any guidance to local transit authorities to ensure cybersecurity is incorporated into their procurement processes.

I look forward to discussing these issues with the witnesses and I yield back the balance of my time.

# # #

Media contact: Adam Comis at (202) 225-9978