# **FDD Media Call:** CSC 2.0 Report on Military Mobility

March 26, 2025
*Featuring RADM (Ret.) Mark Montgomery and Annie Fixler*
*Moderated by Joe Dougherty*

**DOUGHERTY:** Good afternoon and thank you for joining us for today's FDD media call. My name is Joe Dougherty, I'm senior director of communications at FDD, a nonpartisan research institute focused on national security and foreign policy. We're grateful that you've taken the time to join us today as FDD experts will walk you through new research that details the critical US civilian infrastructure -- strategic maritime, aviation, and rail networks, for example -- that the Pentagon needs for military mobility and what the Pentagon is doing and not doing to secure it against adversarial cyber attacks. Joining us on today's call, we have two FDD experts: Rear Admiral (retired) Mark Montgomery, the senior director of FDD's Center on Cyber and Technology Innovation, and an FDD Senior Fellow. Mark is a former policy director for the Senate Armed Services Committee, a former NSC director of Transnational Threats, and served as executive director of the congressionally mandated Cyberspace Solarium Commission.

Annie Fixler is director of FDD's Center on Cyber and Technology Innovation and an FDD research fellow. Annie's research focuses on issues related to the national security implications of cyber attacks, on economic targets, adversarial strategies, and capabilities and US cyber resilience. Some quick housekeeping before we get started. Today's conversation is on the record. We will share the transcript and recording within 24 hours and each of you should have the report in your inbox. If you do not have that, please shoot me a note and I'll get that to you right away. The embargo for the report does lift at 6:00 AM Eastern time tomorrow, and I will shoot you the URL for the report shortly after the call.

Today's run of show is as follows. Mark and Annie will provide the key takeaways of their new report and that is "Military Mobility Depends on Secure Critical Infrastructure." Then we'll open up the call to your questions. During the Q&A portion, you may submit your questions via chat or you may use the raise hand feature, in which case we'll let you know when you've been unmuted so you can ask your question. So let's get underway. Mark, as a retired Rear Admiral, why don't you kick us off by knocking down preconceived notions about how the military moves troops and equipment, how the military mobilizes forces. Does it not rely on its own transport systems for this?

**MONTGOMERY:** Well, Joe, thanks. And I want to thank Joe and the FDD team for putting this on and for the press folks who are on board for listening in and for Annie for co-writing this with me. She did a great job. All right, so no, the military does not rely on its own transportation equipment to get it there. We move and... it's one of these things that, 35 years in the Navy, active duty, I ran plans for EUCOM and the big plans for Russia, the big plans for North Korea, the big plans for China -- I was responsible for each of those at different times of my career. And honestly it did... I mean in my back of my head, I used to hear crazy stuff like, "Oh, the TRANSCOM war plan is unclassified." And I'd be like, "What? It doesn't make sense." Now I get it.

Here's what it is: We use the commercial rail, ports, and aviation system to move our troops, equipment, and supplies forward. And at times you probably have had that realization, but you need to collectively understand that's how we move. Look, the individual elements, like a Special Forces team going to Yemen for something, that's going to be all C-17 from Scott Air Force base, blah, blah, blah. I get that. But for broadly moving our forces, for generating the forces that we need to fight a Russia campaign, a North Korea campaign, or a China campaign, we're going to use our commercial rail, port, and aviation systems 95 to 98%. Why does that bother me? That bothers me because... I'm going to combine this with testimony I gave the House Homeland Security Committee about a month ago where I emphasized Volt Typhoon. There's Volt Typhoon out there and there's Salt Typhoon out there and everyone's like, "Oh, that Salt Typhoon was tough."

Yes, but that was espionage. Volt Typhoon was operational preparation of the battlefield by the adversary. That is the adversary installing malware or cyber malicious activity that isn't necessarily malware into our critical infrastructures. All these transportation ones were hit. Also, power grids, water, a few other things were hit with it, but I'll tell you that was China saying, "Not only do you, Mark, now know that your warfighting is enabled by your transportation systems, but we know and we've done something about it."

The last thing I'll say, because I know Annie's got some good stuff on this, is try to think about this another way: If Volt Typhoon were a thousand backpacks of explosive strapped to our rail system, our port system, our electrical power grid, our aviation control, our airport operating authorities, and it had PLA written on the side with a big middle finger, we'd be at war right now almost, but somehow when it's a thousand cyber malicious packets in these same systems, it's kind of, "Oh, well, give him a hat tip." No, cybersecurity has got to be treated like we treat other, what are considered more traditional military activities. And we've got to defend systems that way, and respond to attacks on systems that way. So this paper was Annie and I describing the problem. She's going to go into some detail on the infrastructures here and discussing the threat and saying, "Action's needed," and we'll get to that in a minute. So pass it back to you, Joe. Joe, you're muted.

**DOUGHERTY:** My apologies.

**MONTGOMERY:** That's our professional press team, guys.

**DOUGHERTY:** Not my first time using Zoom, but it is my second. Well, Annie, walk us through how the military uses civilian-owned infrastructure.

**FIXLER:** Sure, sure. And I just want to thank you so much for organizing this, Joe, and thank you all for joining us today. Just to footstomp that piece on China one last time before we get into the nitty-gritty and the sort of facts and figures about all this various infrastructure. So the intelligence community has repeatedly said that China is pre-positioning assets, that it is conducting these cyber operations in order to impede US decision-making, induce societal panic, and interfere with the deployment of US forces. The recently released annual threat assessment, again, reiterated that just yesterday. The folks of the intelligence community are testifying on that fact right now. So this is a stated... We all know this. How does it actually impact and how is it actually happening in the transportation sector?

So our paper focuses specifically on three subsectors within transportation sector: aviation, rail, and maritime. And so just for a couple minutes on each. So within the maritime systems subsector, the military and the US government has various... They have their own ships. We all know that. We can talk to Mark about the number of ships they have, but in addition to that, they contract with commercial shipping to supplement the ships that they have, vessels that they have. In addition to the vessels themselves, TRANSCOM, Transportation Command has designated 18 commercially owned strategic seaports. These are ports that the military knows it is going to be needing, that it regularly engages with to move forces, to move men and material. So both vessels and ports themselves.

In the aviation sector, it is somewhat similar. There is a voluntary civil reserve air fleet, which is an arrangement the DOD has with civilian air carriers that when they need to mobilize more air assets, they have this with air carriers, airlines. They also have agreements with civilian airport authorities to use their facilities. These are ongoing relationships. It's something in the range of about 70 airports. And then the third piece that's unique in aviation is obviously the air traffic control system. And the FAA is responsible for that air traffic control system. And when military aircraft are flying in US airspace, that is coordinated with the FAA. So that is a also unique component of aviation is that shared air traffic control system.

Shifting over last to rail, the military has its own rail cars, but the rail lines themselves are owned and operated by the freight rail operators. And the US military has designated a network of about 40,000 miles of rail. It's about a third of the whole rail network and it calls that the Strategic Rail Corridor and that is the rail lines that the military knows it is going to need and uses on a regular basis to move from various military facilities to ports, between military facilities, et cetera.

So those are sort of the different components. And these are longstanding relationships. They are existing systems, but those are mostly focused on the availability of those assets and not their cyber resilience. The cyber resilience component of it is solely or the majority of the responsibility for that lies with what are known as Sector Risk Management Agencies. Those are federal civilian executive branch agencies that work with the private sector on a regular basis to identify and mitigate cyber risk. And our concern is that that effort is siloed from DOD's efforts. DOD has critical infrastructure protection programs, but they do not talk necessarily very well to Sector Risk Management Agencies. And so our concern is that the DOD does not have a good understanding of the risks that the transportation system sub-sectors are facing.

**MONTGOMERY:** Let me jump in on that too and just say, part of this is that the DOD does a good job taking care of their bases. I like to say ... Annie's heard me say this, that you're on a DOD base, there's two comms networks, two power systems. One of them might be a CATL battery from China, but we'll ignore that. Two water systems. It's like the Noah's Ark of critical infrastructure, and that rail car leaving the base ... got the tank on there and it's leaving and it enters like Norfolk Southern. And that's like Mad Max Thunderdome, right? Now you're on your own in that cybersecurity world. And the DOD has worked very assiduously, very hard, and very skillfully to only own the base. They'll study the immediate infrastructure of the base and how it supports the base, but then when it goes out to these ports and aviation and the rail system to get there, not their problem.

Now look, let's be clear, they care, but they don't care enough because they don't want to get the bill. And that's what it always comes down to. DOD says everyone sees us as like Moneybags McDuck there and we've got ... and if we show up and say we're here to help, we're going to end up paying the bill. So what I really think has happened here is the DOD has done a great job making sure we can kick the bejesus out of any adversary that attacks a military base. But if we got to go overseas, they have not worked that ligature to be successful. Joe, back to you.

**DOUGHERTY:** Thanks, Mark. Thanks, Annie. Can you talk a little bit about how the military, in addition to using civilian-owned infrastructure, we're going to talk about some of the threats that Mark discussed at the outset and particularly the subsector? So you've got Chinese-made ship-to-shore cranes, you got the rail and the supply chain problem, modernization of air traffic control system. Can you talk a little bit about that?

**MONTGOMERY:** So I'll pick up, thanks with the first one with the ship-to-shore cranes. Now look, I want to be clear, I'm glad that Representative Garbarino and then later the China Select Committee really highlighted the crane problem. But I want to make it clear. A modern port system, our 19 containerized ports, so the United States has about 60 ports on the East and West Coast and Alaska, but 19 are considered big ports, ones that have containerized loading of ships. You know, you see the stacked up containers that go right, or big LNG, or other kind of facilities. A couple of those are owned by the military in Charleston and in Oakland, but 17 of them are owned by the private sector, operated by local authorities usually, either owned by the local, state, or county or by a private sector company there. But it's more than the cranes in there that are automated. The gantries that move these things along, the gates that open, the rail cars operated. It's all automated. When you go and watch this, it's impressive.

There's some humans on them. These are kind of union rules if you ask me, but in any case, there's humans on them to take over if necessary. But the vast majority of it's automatically operated, the speed they go at. And there's men and women doing the safety lines, stevedores and stuff. So there's legitimately workers there.

But the actual movement of things is highly automated. By the way, you need a really good GPS system for that because you have to know exactly where you are and exactly where that sea/air/land container is. Anyway, so don't just think cranes. However, when you look at the cranes, you have a couple of, "Oh my God" moments like, "Oh my God, every crane's made in China." 90%, but still these big huge cranes you see at them, there's four or five at every port. So there's a 100+ in America, around a hundred in America. I think 85% made in China, maybe 90%. In any case, it's not the cranes... And the Biden administration did this executive order, said, "We're going to fix this problem and replace the cranes," which sounded good to some probably blue state crane manufacturers like, "I'm going to build some expensive cranes here." That's not really going to happen. We don't need to replace the cranes. We need to replace the brains in the cranes. They cannot come from China, they can't be continuously software-updated in China. They're cellular modems, which is a future Huawei problem. The cellular modems of America are about 40 to 45% Chinese-made. That's what talks back and forth with China. That stuff needs to be inspected, assessed, and over time, transitioned to American or ally and partner equivalent systems, the brains of the crane, the cellular modems, that's a much smaller problem than replacing $100 million cranes, right? So we got to get that, to be the cranes, you got to do the same with the gantries and the other stuff.

Now just mention here, the Biden port executive order was a great executive order if only there was money to do it because as we all know, executive orders don't come with cash. It assigned the US Coast Guard a ton of really important things. I'll stipulate every one of them was a good idea. The problem, of course, is that there's no money and the Coast Guard was already a service that didn't have two wood nickels rubbed together and you're telling them to go do this. And because they're a military service, they're trying to do it by not doing ...

But in the end, do you want the Coast Guard to rescue you when you're lost at sea or do you want them doing crane inspections? In the end, the Coast Guard defaults to rescuing you out at sea because that tends to be a bad news day if you don't, whereas the crane inspection isn't noticed. So we've got to get them money so they can do the crane inspections separate from rescuing people out at sea.

So from my perspective, if the crane's issue is a money issue -- I know I went long there, Joe, but I just want to take one of them and really draw it out. Annie, over to you.

**FIXLER:** Yeah, sure. I'll touch on the other two. The first point I'll touch on is rail. And so rail has a similar ... not exactly the same, but a similar supply chain problem to the ship-to-shore cranes that Mark was speaking about. China makes a significant amount of rail cars. And these rail cars similarly have a lot of sensors and equipment to make sure that they're temperature-controlled or that the operator knows exactly where they are. That they're not sort of just a box on wheels. They're a very sophisticated piece of machinery. And so China has been attempting to penetrate both the freight rail system and the passenger rail system and to be a larger and larger manufacturer of of rail cars. Luckily in the past couple of years, Congress and successive administrations have gotten wise to this. And so as part of the Bipartisan Infrastructure Law, Congress passed some rules and the Federal Railroad Administration has issued some regulations to prohibit the purchase of new Chinese-made rail cars. And that has been supported by the US rail car manufacturers.

But that is a step in the right direction that does sort of begin to address the problem. It doesn't necessarily address the existing rail stock, nor does it address the maintenance of the existing stock. So that is an ongoing problem that needs to be addressed. Again, because they are such digitized systems, they provide a lot of intelligence capabilities. If China knows where its various rail cars are going, it has early warning of US efforts to mobilize forces. So that's sort of a piece on a problem in rail. There are many problems in all of these different subsectors, but just to highlight another component of aviation is the modernization of the air traffic control system.

Some of you may remember back, I think it was like November '22 or so, there was an incident in the FAA's NOTAM system and the system went down and so flights were grounded for a couple hours. That was not a cyber attack. We all know that was not a cyber attack. What that was is just a misconfigured file, like the deletion of a file from one folder and moved it to another. That's a problem. That is a failure of a system that is that brittle, that that will take down a whole network, that will take down a critical component of air traffic control and have to ground flights. So that system needs to be modernized and made much more resilient. And so that's one of the pieces of concern as it relates to the aviation subsector.

**DOUGHERTY:** Thanks, Annie. Mark, you had mentioned GPS. Let's come back to that for a second. How is that relevant to the discussion and why is the current situation a problem? And Mark, maybe you can address it and Annie can talk about critical infrastructure and how it uses GPS and then we can turn to Mark for a deeper dive on DOD's failings.

**MONTGOMERY:** Yeah, so it had GPS. Look, we added this in, honestly, we were moving along on this and then I experienced two things. One, I think some of you know on this, I go to Ukraine and train their operators there. And we are seeing very explicitly in Ukraine that the use of jamming by the Russians has prevented some munitions, GPS-enabled munitions like Excalibur for not working that well, particularly when it's coming into a localized area, like 155, like artillery rounds. Okay?

The second thing is you travel to Israel, which I do frequently, and I go up north near Lebanon and suddenly my GPS tells me I'm in Beirut airport. If I go south towards Gaza, it suddenly tells me I'm down in Cairo airport. My suspicion is that the Israelis are spoofing GPS because if a drone thinks it's in an airport, it lands, right? So they're trying to spoof inbound drones.

In addition to the jamming and spoofing problem, the overall GPS signal in our iPhones -- but just by the way, same GPS in here, little antenna -- it's also in the crane, it's also in a John Deere tractor, it's also in the railroad car. It's also in everything else in infrastructure. Our critical infrastructure relies on GPS, just like the military relies on it. Our signals are getting weak. If you drive around downtown San Francisco or New York City, you've noticed this, that it's even in DC sometimes it has trouble tracking you. That's our weak signal. And it's in a tough environment like an urban environment starts to show its weakness.

Many of our phones shift over to Galileo, the European stronger signal, or if your phone's not being operated properly, which most of yours aren't, it could go to GLONASS, the Russian system. Congratulations.

All right, so what we're doing is we're shifted. We saw this 20 years ago. We're not stupid most of the time, and we put up two satellite systems called GPS 2F and GPS 3, and they came together to make the next-gen GPS system and that uses an antenna called the L5 antenna. The L5 antenna, 30 times more powerful. You're in San Francisco, no problem. By the way, when you're in your remote driving car in San Francisco. I really want that. Right? Then also all the tractors out there in the middle of nowhere land, that'll work great, right? The ports, it'll be great. Our war fighting systems would be much safer and it's 30 times harder to jam. Instead of a jammer having to be the size of a suitcase, it has to be the size of an 18 wheeler. Tough to mask your 18 wheeler down by Norfolk Port as opposed to your suitcase jamming device.

Bottom line is we need to shift over and you say, no problem, Mark, we've got 18 of the satellites up we should -- by the way, only because we put legislation in that forced the launch of the 18th, the Space Force was so slow on this. Then, of course, there's a problem. The problem is Raytheon is supposed to deliver something called the Next Gen[eration] Operational Control System, was supposed to come in 2022, then 2023, then 2024, and then spring of 2025. It's now fall of 2025. We need to make sure that system comes online because once it is, it's controlling these 18 DOD, and the Department of Transportation can certify it to do anything except flight safety, flight safety, it's 21 satellites, don't worry about that. But for all the other things, it could really help us have a better GPS system and then that L5 antenna will be in your iPhone 17 or whatever and in your other systems. I'm excited that we're close. I'm disappointed that we could have been here three years ago. We got to continue to get that worked out on GPS.

**FIXLER:** Yeah, thanks, Mark, for that set up and for the detail of how fragile the system is at times. I just want to spend one more moment on how it is used in critical infrastructure. I'm sure we're all sort of aware of the navigation component, the position component of GPS. I just want to spend a little bit on the T in PNT, timing. In addition to the use on position navigation, GPS systems are also used for the timing of, for example, generation facilities for the electricity subsector. You need to get generation facilities in sync so that your electricity doesn't get out of phase and you don't create huge problems in the system. Companies use GPS for that capability in the financial system. GPS is also used for precision timing of trading, things like that.

In the communications system, similarly, you want precise timing on communications systems, so they use GPS for that. All of these are just different ways that companies in the private sector are relying on this asset that is a sort of, at this point a public good, right? It is originally a DOD constructed system, but it is, the critical infrastructure relies on it. We participated, a couple of us from our team, participated in a tabletop exercise last fall looking at critical infrastructure resilience and how the private sector and public sector work and the government work together. Our game designer, the first thing he wanted to do was jam GPS because he knew that that was going to cause a huge problem for all of our different critical infrastructure players, and so that's what he did, so it's not hard. Our adversaries know that. We know that. We need to fix this system to get it to be much more resilient.

**DOUGHERTY:** Let's move over to PNT. Can you talk a little bit about that, Annie?

**FIXLER:** Yeah, so that's the position navigation timing, the "t" is that timing piece of PNT.

**DOUGHERTY:** Very good. Mark, you all talked about the current situation as untenable. So let's talk solutions. Your paper has about a dozen, if you don't count sub bullets A and B in many of the recommendations. Can you give us some of the highlights of your recommendations?

**MONTGOMERY:** Thanks. I'll do that and then I'll do a little bit, and then Annie can wrap it, and we go up to questions then. Look, what we did was like we normally do here, whenever we finish -- the FDD, we like to fashion ourselves a "do tank" -- so when we write a policy paper, we write detailed recommendations including draft suggested or draft sample kind of legislation that we would've wanted. Then if someone asked for it, then our FDD-A will go ahead and provide it to them. The bottom line is there's a number of areas here where you can either do authorization work or appropriation work. I'll highlight two. There's grant programs. Look, we're not talking about if Atlanta Hartsfield and Chicago O'Hare have a cybersecurity problem, I'm not interested in helping them fix it. They collect so much darn money from me when I pass through their own taxes, I know they got money.

When I go to Columbus Airfield, Columbus, Ohio, the airport there, that Air Operating Authority run by the county, now they're not getting a lot of tax money and they've still got to maintain these airports and maintain them to a standard the military needs for other things, but also for themselves and for FAA flight safety, all that. Now, I turned to them, they're going to need a grant program. They're not going to get healthy. If you do more on cybersecurity, they're going to do less on making sure the tactical aid to navigation is at the right power that keeps planes from hitting each other. I want the radars working there and everything. To fix the cybersecurity, we want a grant program. It says, look, if you're assessing to a standard that DOD says they need and you find a gap in meeting that standard, and then you bring us a request for funds, we'll get you a grant.

Now, this isn't for the overall modernization of your IT system. We're not doing that. If you're on Windows 7, that's on you, but if you are talking about specific cybersecurity vulnerabilities that you identify and try to meet a DOD standard, this kind of grant program will help. There's a couple grant programs in there, and I'll do one other. As I said earlier, only as I mentioned earlier, the captains of the port, the Coast Guards have these guys called -- and men and women called -- captains of the port at each of the major ports. They're Coast Guard 06s for the most part, or 05s, captains or commanders who actually provide a lot of safety and inspection support already to the ports.

They're doing cybersecurity out of hide right now. They need specific funding for cyber professionals that's put in the budget so that the Air Force doesn't have to have the person also doing inspection for HAZMAT doing cyber on the side, or one less person inspecting HAZMAT than was supposed to be, so that you can inspect for cyber. We want to make sure these captains of the port have the right kind of people. There's some funding for that. It's overall about how the Coast Guard is an effective sector risk management agency. Annie, one or two more from you?

**FIXLER:** Sure. Yeah, so first things first, we can't talk about more cybersecurity standards and regulations without talking about regulatory harmonization. Each of the industry associations associated with the various subsections we've talked about have shared information with the federal government, had issued statements publicly about their concerns that various regulations that they're facing are not in harmony, that they are conflicting or duplicative. Recommendation number one, let's get this organized correctly so that companies are not spending valuable cybersecurity dollars constantly proving to yet another regulator that they are indeed cyber secure. There are important reasons to have minimum cybersecurity requirements, but let's get those in sync so that companies have less of a burden but can actually spend the money on the cybersecurity itself. That's point number one. Also, you'll hear a lot from us, we do love an exercise, a tabletop and a live fire. We have previously talked about the importance of doing exercises around military bases when it comes to their resilience in energy, water, and telecommunications.

Congress issued, that was part of a previous NDAA, not sure that the military has done that the way that we would want them to do those exercises. Not sure they've actually accomplished those, but in addition to that, yet another exercise, we need to actually test the systems when it comes to transportation. Do we have the resilience in the system? If there is a cyber incident, as there likely would be during a hot conflict, do we have resilience in the system to move in a different way or to operate through crisis? More exercises between the military and the private sector, both at sort of the local level and at the national level.

I will just do one more. There are lots of recommendations, as Joe said, there's a dozen. So I mentioned STRACNET, the Strategic Rail Corridor [Network]. The DOD does an assessment of that. They issue it every five years. They are assessing that they understand the networks they need. There's no indication that cyber is a component of that assessment. It seems like that's a logical place where we can do a little bit of an adjustment and have a really significant impact if DOD looks also, through a cyber lens at the resilience of that system. Doing some sort of cyber assessment of STRACNET would be, I think, meaningful when it comes to rail. Joe, back to you.

**DOUGHERTY:** Yeah. One last observation. We've done several of these media calls on your terrific research -- "cyber on the side," it seems to be a theme, whether it's rural hospitals or water utilities, DOD and critical infrastructure. Just want to address that overarching theme of cyber on the side and the need to do better there?

**MONTGOMERY:** I'll go. Yeah, I mean, this is what we, Annie and I, are looking at, I mean, our goal at CCTI and CSC 2.0 is to look at all 19 or 20 critical structures because as you know, transportation's broken up into a few. As we do that, it's very uncommon that cyber is seen as a primary mission by the people we're talking to. If a federal agency doesn't have the name cyber in its name, like CISA or Cyber Command, cyber is a side dish. In fact, sometimes it's like a ketchup. I mean, it's a small side dish. And so the government needs to do a better job. The enemy knows this. The enemy does not see cyber as a side dish. They see it as a vulnerability that they can attack and they're hitting us hard.

**FIXLER:** And that side dish component is reflected also in the private sector. Cybersecurity, I would like to say the narrative is changing, but for far too many companies, in far too many sectors, cyber security is a cost sink. It is not seen as critical to business operations, even though it is. And so our recommendations, usually the recommendations you'll see at FDD are really focused at the federal government level, sometimes state level, but we know where our sweet spot is. But that doesn't mean that the private sector itself doesn't need to do a lot of its own work.

**DOUGHERTY:** All right. Let's transition over to the question and answer portion. So those of you on the call, you may ask a question one of two ways. You can raise your hand, use that feature or you can jump in the chat and type in your question. My colleague Ellie Bufkin is in the background making sure that everything goes smoothly. In the meantime, any other recommendations that you wanted to emphasize to the reporters here?

**MONTGOMERY:** I think that's most of them. We'll see if we got any questions here.

**FIXLER:** I will just spend one more moment while folks are thinking of their question, I will spend one more moment on the grant program and I will hit on the rail sector because it's a little bit -- this report goes through three sub-sectors. You'll recall or maybe you won't, but I will remind you that about two years ago we issued a report looking at more in depth on the port sector itself, the port sub-sector itself. And so we are also ticking through, doing longer reports on the other two, on aviation and on rail. And so I have been doing a little bit more digging into rail in addition to this paper. I have another colleague who many of you know, who I'm happy to put you in touch with if you don't, who has been doing a deeper dive onto aviation. So look forward to that coming out relatively soon. On rail, since I'm going to spend a another moment, the grant program, as Mark mentioned, there are really large companies in the freight rail sector. These are class one freight rail companies. They're billion-dollar companies. The amount of money that the federal government could give them, to cybersecurity, is pennies compared to their budgets. But there are a lot of very small rail operators, short line rail operators, who a small amount of money could make a meaningful difference to their cybersecurity budget. So our recommendations when it comes to federal spending, really focus in on where could we have a meaningful impact with a small number of dollars. So that's just a little bit more background.

**DOUGHERTY:** Very helpful Annie, thank you. Our first question comes from Sarah Friedman at Inside Cybersecurity. Sarah, over to you. You are unmuted.

**SARAH FRIEDMAN:**... to ask more about the appropriations and providing grants and funding for opportunities. Right now we're in an environment where people don't necessarily want to spend -- appropriators and lawmakers don't necessarily want to spend more money on creating new programs or authorizing new appropriations. Are there any grants that you think would have the most impact that you could highlight?

**MONTGOMERY:** Yeah, so I'll go first and Annie can follow up. So I agree with you, but I also say one of our other options here is to have DOD take this over. And if I've learned anything in 35 years in the military, is that having DOD run something inherently makes it more expensive. So I just think what we're offering here, I think is the most cost-effective and efficient opportunity. And also one other thing, if you were to ask me, "Hey Mark, which of these sectors, overall in America, is in the best shape?" I'd probably end up saying it'd be financial services or energy. And the financial services at the big bank levels, because they spend a billion bucks each on cyber security, because they're getting attacked and robbed, and they bake that in for three or four decades. Energy though, part of it is that we run a robust energy grant program inside the appropriations for the smaller and the rural ones, and that's made a big difference.

So I would say grant programs are one of the best ways to tackle this, if properly understood and utilized. So I'm pretty excited about grant programs that are done right, and this would be very targeted. There's 60 plus airport operating authorities that could get at it. Really, there's several dozen rail things to get. There's seven big rail companies, but really there's smaller rail, people who own aspects of rail, but it's a targeted number. So I think you could inform them about it, make decisions on how well off they are, and that, you know, needs-based test it, and then provide the support. I'm pretty comfortable that there's a good opportunity here. Annie?

**FIXLER:** Yeah, just to say sort of two additional sort of points to make. One, there are existing grant programs that are security focused. What they aren't is cybersecurity focused. So if we can sort of build on momentum on security focused grants or even, I mean our recommendations are for new grants, but there are ways to make them to adjust existing grant programs to say, "and cybersecurity" or "and prioritize cybersecurity." So there are alternative ways to do it. We would argue for a new program, but there are additional ways. The other thing I will say is we like to make recommendations that we think are doable, but we are also going to make recommendations that we think are appropriate, and we are going to push forward recommendations that we think are appropriate regardless of the political climate. In recognition of the political climate, but regardless. I like to sort of lean back to or look back on the Cyberspace Solarium Commission and when they issued their report. There are a number of recommendations in that report that as they were issuing them, including things like "make a cyber committee in Congress" that they knew there was no political appetite for at the moment. It doesn't mean there won't be a political appetite in the future. So you'll still see recommendations out of us that sort of come both ways.

**DOUGHERTY:** Mark, I suspect some of the reporters in the call here today would be curious on your thoughts on Capitol Hill and if Congress is aware of these challenges, and any suggestions that you might have on next steps based on your research?

**MONTGOMERY:** Real quick, I do spend a lot of time talking to about this, and this is one of the hard parts about this. We haven't said it completely cleanly, but one of the problems in the executive branch is, this is interagency, right: Coast Guard for the ports, TSA for rail, TSA and FAA for aviation, DOD for DOD. It's equally clustered up in the Congress. You've got the House Armed Services Committee, but they care about this, but they really don't own any part of it. It's owned in the House, in E&C, Energy and Commerce, T&I, you know, Transportation and Infrastructure, House Homeland. In the Senate, it's owned in Commerce, Science, and Transportation. It's spread out into, and as well as SASC and Homeland, or HSGAC in the case of the Senate. So in each place it's owned in three or four places. It doesn't lend itself to easy usage of the NDAA except maybe by floor amendments. So we'll have to see what happens this year with all of our recommendations. I'm hoping to see a few in the NDAA and then a few more in the markup, and then a few more in the floor amendments, but a bunch of them are going to have to carry on other language and that's hard.

**DOUGHERTY:** Very good. I think we'll end it on that, although I will ask Annie and Mark to provide maybe a 30-second summary. In the meantime, I just wanted to thank everybody for being on today's call. Mark and Annie, as well as the journalists on today's call. I want to thank Ellie in the background for making everything run so smoothly. Again, the embargo lifts tomorrow at 6 AM. If you do not have the PDF of the report, please email press@fdd.org, and we'll get that to you right away. And I'll also be getting you the URL that you can insert in your coverage in the meantime. You can always reach the press team if you want to talk with Annie or Mark, reach us at press@fdd.org. Okay, so some wrap up thoughts, we'll go to Annie and then go to Mark.

**FIXLER:** Sure. Just to reiterate Joe's comment that if you have additional questions about this report or any of the topics we've covered here today, please do reach out to Joe and the press team. We're happy to provide some follow-up information. The main thing that I would continue to foot stomp when it comes to critical infrastructure security is the importance to national security. We all talk about critical infrastructure as important to national security. That's sort of in the definition of the name critical infrastructure security. What we hope we've communicated today and what we hope the report communicates, is not just this vague sense of national security, but that critical infrastructure, resilience and security is a key component and essential to military readiness. And so it is not vague, it is core to our capabilities. Mark, your last thoughts?

**MONTGOMERY:** Well, China's got this figured out. I hope we can get it figured out. That's all I'm thinking. Go ahead, Joe.

**FIXLER:** I got you, Mark. Thank you. Again, thank you to everybody on today's call. This does conclude today's call.