FDD EVENTS

Cyber Catastrophe Recovery: A Critique of U.S. Continuity of the Economy Planning

Featuring Rep. Andrew Garbarino (R-NY), Tom Fanning, Mark Harvey, and RADM (Ret.) Mark Montgomery
Moderated by Dr. Samantha Ravich

RAVICH: Thank you all for joining us today. I'm Samantha Ravich, Chair of FDD's Center on Cyber and Technology Innovation. It is Wednesday, September 13, and today we are joined by Representative Andrew Garbarino and Tom Fanning to discuss Continuity of the Economy, a key feature of how we ensure the resilience of our country and thereby deter our adversaries.

The strength of a nation's economy shapes its military power, national security, and international influence, and that is why we should expect our adversaries to try to attack our economy using cyber or other means to undermine U.S. strategic power and constrain our options.

Congress recognized this, and in the FY 2021 National Defense Authorization Act, Congress required the President to develop a Continuity of the Economy, or COTE, plan to maintain and restore the economy in the wake of a devastating cyber or kinetic attack.

COTE planning isn't easy. Critical infrastructures are highly interdependent. The digital ecosystem on which our economy depends is not controlled by the federal government. Understanding and determining the order of recovery involves rapidly synthesizing data, deploying infrequently used emergency authorities, and working closely with the private sector, something the government does not always excel in, especially in emergency response situations.

Again, Congress was not blind to the challenges, and so it gave the Biden administration two years to develop a plan, or even a plan for a plan. What Congress got however was neither.

To discuss the challenges of COTE and what needs to be done, we've brought together a panel discussion today of experts from Congress and private industry, as well as experts on resiliency and continuity planning.

First, we are pleased to have with us Congressman Andrew Garbarino from New York's 2nd District. Representative Garbarino has been engaged on Continuity of the Economy issues for many years and now sits at the perfect intersection to move the needle on this topic, serving as Chairman of the House Homeland Security's Committee Subcommittee on Cybersecurity and Infrastructure Protection and as Vice Chairman of the House Financial Services Committee's Subcommittee on Capital Markets.

We are also joined by Tom Fanning, Executive Chairman of Southern Company. I had the privilege of serving with Tom on the Cyberspace Solarium Commission, and he is precisely the kind of thoughtful, knowledgeable, patriotic private industry leader that the U.S. government needs to be engaging with COTE issues. He served for a decade as Co-Chair of the Electricity Subsector Coordinating Council and Chair of CISA's [Cybersecurity and Infrastructure Security Agency] Cybersecurity Advisory Council.

As I said before, the administration belatedly relayed the response to Congress, but long before that, it became obvious to those of us who were watching closely that the administration was not setting itself up to provide a robust response to Congress.

So here at FDD, we didn't wait for the administration to do its required work. We knew that we couldn't wait. Not only is a COTE plan crucial for our continued way of life, but the adversary must know that if our economy is attacked, we can get up the next day, defend ourselves fully and completely. It is a key plank of deterrence.

And so we've been working ever since the passage of FY 2021, the National Defense Authorization Act, to develop research and pilots and playbooks to help the ball move down the field, which is why we are so pleased to connect with Mark Harvey, one of the smartest people on resiliency planning I've ever met. Mark has served in both the private sector and in government, in continuity planning positions and on the National Security Council staff. He is co-author of our new report, “After the Attack, a Playbook for Continuity of the Economy Planning and Implementation.” The report is available on FDD's website and there is a link to the report directly on this event page.

Lastly on this panel, we will have Mark Montgomery. Mark serves as a senior director here at CCTI [Center on Cyber and Technology Innovation] and also directs CSC (Cyberspace Solarium Commission] 2.0. I met Mark when he was executive director of Solarium. Mark served for 32 years in the U.S. Navy, retiring as a Rear Admiral in 2017.

Following the panel discussion, we will be taking question-audience Q&A and encourage those who are watching live to email questions to events@FDD.org or to tweet them @FDD.

One last piece of introduction before we jump into the discussion, a few words about FDD. For more than 20 years, FDD has operated as an independent, non-partisan research institute, exclusively focused on national security and foreign policy. As a matter of pride and principle, we do not accept foreign government funding — never have and never will.

So with that, let's jump into it. Congressman, thank you for coming. You have — really, you've been a force in Congress to get the administration to fulfill their legislative requirements and get Continuity of the Economy planning going.

And, you know, I found that it's not a topic that most people care about or even understand, and yet as a freshman Congressman not a year into your first term, you started writing letters to the administration about this topic.

You seem to appreciate in ways that others do not the danger of not having a plan for what we do if we face a major cyberattack on multiple critical infrastructures at the same time. Given your unique position on your committee, what is it about the COTE issue that first resonated with you? And why have you decided to focus on this issue as part of your public service?

GARBARINO: Well, Samantha, thank you for having me today. And everybody, thanks for joining.

You know, it was — I'm from New York, I'm a member from New York. I was in high school when 9/11 happened, and that was the last time really, you know, we were attacked on our soil. I don't see that happening again. You know, we have really done a lot to protect against that, an actual physical attack from a foreign nation. I don't see Russia invading us like they've just done with Ukraine.

What's going to happen is going to be cyberattacks. That is the next step, that's the way people can get to us. So we need to step up our game and protect against that. And if they're not going to physically be dropping bombs on us, they're going to be attacking our critical infrastructure sectors. Financial services, pretty much based out of New York City in the United States, is one of the top critical infrastructure sectors. There's energy, there's transportation, there's healthcare, there's all of these that we need to protect against. And it’s not even that they're going to attack us, specifically attacks against us, you know, there going to be another nation state going into, a NATO ally. They might tech — attack us to keep us out of it.

This is — we have to prepare for this, and the fact that not everybody's looking at it — look, I didn't know anything about it before I got to Congress, and — but it's like, it's scared straight. You know, I — once I was told, I said, "We've got to get — we've got to get moving on this." And the fact that the administration dragged their feet for so long after legislative delegation, I mean, we passed it in the NDAA. It said they had to do this. We got an answer eight months late. You know, they — and it was pretty much set up to fail from the beginning. They — they took forever to designate CISA as the lead agency on it. It's like they're not taking it seriously and that scares me.

And I you know, on the past couple letters, I worked with Chairman Gallagher, who I know, you know very well, and a lot of people know very well. He's also very concerned about this. So there are — other than myself, there are other members in the House and the Senate that are focusing on this, but we really need to step up our game and make sure that, you know...

And it's not just going to be one attack. Like you said, it's going to be across several sectors, and we need to be able to make sure the government and the private sector are moving equally to get things up and running again because if our economy's not running, if our transportation's not running, if people can't get on their iPhone and watch TikTok, you know, things are not going to go very well.

RAVICH: Well, we'll get back to the private sector in a moment, but I understand your subcommittee has been taking a close look at CISA's role as a national coordinator and as a sector risk management agency, SRMA, for eight of the 16 critical infrastructure sectors. That's what you cover. And you've mentioned that your subcommittee intends to pursue additional oversight to refine CISA's public-private partnerships. What do you see as CISA's role in Continuity of the Economy scenario? What do you see as each of the SRMA's roles? I mean, talk to us about that and talk to us about, you know, your oversight of that agency and the 16 of — eight of 16 critical infrastructures.

GARBARINO: Well, yeah, we have been doing a lot of oversight with CISA. We work — we do work closely. I have a very good relationship with Director Easterly. She and I have had several meetings. We text back and forth. I have faith in CISA. I got a — you know, my predecessor — one of my predecessors on this comm- — actually, on this committee, was John Katko, who was very supportive of making sure CISA had what it needed to do its job.

I'm happy that CISA is the sector risk management agency for eight of the 16 critical infrastructure sectors. I'm concerned — you know, I think it's more mature than some of the other agencies that are tasked with being sector risk management agencies. So I think there's other agencies that have room to grow. I don't — I don't want to name them here and throw them under the bus, but I — you know, I could give you a couple.

CISA, though, from all the work I've done on this committee over the past two and a half years, I think one of CISA's biggest strengths is its ability to have its public and private partnerships. The private sector, from what I've been told from most companies, prob- — almost all, is they really do enjoy working with CISA compared to other agencies. So there's a level of trust there, so the — I think that's — that's a good base to have, you know, to build off of this — you know, build off of COTE — you know, to build COTE off of.

So you know, we're going to continue to do our oversight. We're having another hearing next week to hear from private sector about, you know, what CISA's doing right, what CISA could be doing better, and then we're going to have a follow-up hearing with CISA to have and take questions on that. But you know, when it comes to specifically sector risk management agency and CISA, they've got to update their plans. All the other agencies have to update their sector-specific plans. But they're all waiting right now for the administration to update PPD 21. That's taking way too long, and nobody else can move until the administration updates that directive.

RAVICH: Well, maybe you can talk a little bit more about, you know, about what you see as what's stalling it, why it's important to update it for all the work you're doing, and again, not just, you know...

GARBARINO: What's stalling it?

RAVICH: ... this is like — about capital markets. You know, you really, again, you sit at this intersection.

GARBARINO: Yeah, I sit at the —and unfortunately, I think what's stalling it isn't necessarily — I think it's — I think there's — you know, I think there's a couple of different people. I don't think there's a clear person running cyber out of the administration. I think there's competing — I think there's competing individuals, which is causing things to be delayed. I think that's why we also had a — why our COTE plan that just came out for — of the administration wasn't a plan; it was, "Hey, by the way, we've got this thing taken care of Don't worry about it."

I think right now, I don't want to say egos are — competing egos are the right word, but it's, you know — I think that's the issue. It's not bureaucracy as much as it is, "I'm in charge." "No, I'm in charge." "No, I'm in charge." And no one's making an actual determination of what to do. And at the end of the day, we're all going to — we're all, you know — by doing that, they're not answering what Congress directed them to do, and by the way, which was also signed into law, though. I mean, they're not answering what Congress directed them to do, and the private sector's out there — the private sector who owns, by the way, 80 percent of the critical infrastructure, or runs 80 percent of the critical infrastructure, they're out there waiting to, like, "Alright, who are we working with? What are we doing, you know, in case of all this happens?" The — there's no guidance there, so it's a — it — there doesn't — there — there doesn't seem to be — it's not one — there's not one person making the decision. There's — it's like a couple-headed monster there. And I went on a little ramble, but it's just — it's very frustrating.

RAVICH: Yeah.

GARBARINO: And we've had this conversation privately...

RAVICH: Yeah, no, no, it is, and that's, I think, what's led up to this less-than-stellar, you know, report that's been handed over to you. But you know, sustaining vital economic functions during a crisis really requires collaborating with certain private sector partners. I mean, that's what you were just talking about, since they're the ones, you know, providing critical economic services. And you have been a champion on making sure that the private sector voice is heard not just on COTE, but on cybersecurity issues, you know, more generally. So I mean, talk a little bit more about, you know, how you think that private sector, private-public collaboration is going in, you know, in a broad sense. Is the private sector being brought in to inform decision-making processes?

GARBARINO: So I — look, like I say, the private sector, everyone seems — from what they're telling me, they really do enjoy working with CISA.

RAVICH: Um-hmm.

GARBARINO: You know, energy — and the energy companies love working with DOE. You know, they have — for most of — for the most point, but when it — you know, the one thing we've heard with, and it's not CISA; it's other companies, because I don't want to — this is not — the COTE — and I don't want to lay blame on what we just got with COTE on CISA. It's not their fault. This was — this was coming from the administration. I don't think this was — I think CISA was set up to fail, with what — with the timing and everything that was done here.

But when it comes to information-sharing discussions, the relationship seemed to be there with CISA. So I think CISA should have a bigger role when it is — when COTE is finally determined and there actually is an actual plan. Because those relationships are already there, and we can build on them.

The problem is, from what we've heard, is information-sharing, a lot of the times it's not timely. It's one-way. So that has to be fixed. But whatever happens, whoever's running it — say it's not CISA. You'd — like 80 percent of critical infrastructure is owned by the private sector. If, all of a sudden, we have an attack where the banking sector goes down, the healthcare sector goes down, the transportation sector goes down and the energy sector goes down, it's not going to be somebody in Washington, D.C. in a room getting it back up; it's going to be the front line are going to be those private companies.

They're going to be the ones out there fixing everything and making sure it — everything gets up and running again, in hopefully a short amount of time. Look, there has to be — there has to be communication between the government and these agencies. You need to be working with, you know, local law enforcement and emergency services. You know, this all has to be done together. But the private sector, it's going to be their employees, who are going to be getting their systems back, nobody knows it better than them. They're going to be the ones who are tasked with getting their system back up.

So it doesn't do us any good if there's no relationship there. So we — you know, you can't have it — you can't have a COTE plan — I mean, I guess you could; it wouldn't work. But you can't have a COTE plan unless there is that public-private partnership. And I'm not even sure — and, again, it's one of those things where I don't think you could have a — and this is something we can talk about – Tom might have an opinion. But you can't have a banking-sector person then telling the energy sector what to do. Every sector has to have its own leader.

It's — but you have to have that relationship, that public-private relationship, or we're not going to be able to stop anything, you know. It's— and you look at...

RAVICH: Um-hmm.

GARBARINO: You look at what happened, you know — I mean, it's just — you know, I can keep going, but I know we...

(CROSSTALK)

RAVICH: Yeah, and you, kind of — you know, again, I think you stated it perfectly. And, I mean, with your broad oversight of, you know, some of the most important parts of our economy, sure, I mean, they are responsible for their piece of it, but it is the coordination of how they all work together.

We've seen this since we started writing here at FDD on cyber-enabled economic warfare, you know, five, six years ago, running various sectors — bringing them together and running them through "What if they're all attacked at the same time," understanding the interdependencies. They do — they're getting to, but they need a traffic cop in some ways, right?

GARBARINO: Um-hmm.

RAVICH: And there will also be very large amounts of federal aid assistance and direction because, most likely, let's face it, if there is a major cyberattack across critical infrastructures, it's not going to be, you know, most likely, a naturally occurring event, and...

GARBARINO: No.

RAVICH: ... that's where — that's where this all comes in.

GARBARINO: And, by the way, you know, it's —and I was reading this Politico article the — yesterday, it was. It's not even just about foreign nations; I mean, we have — there are — Politico did an article about climate extremists attacking the — several parts of the electrical grid, both physically and by cyberattacks, in multiple areas, to try to cause blackouts.

Like — I mean, we have — this is a huge issue. And it's not just like, oh, we've got to plan on what, you know, China's doing; we've got to plan on what Russia's doing, on Iran, North Korea. You know, we've got people in our — who might have one issue that they're focused on that might be — that are taking this stuff into their own — so we've got — it could be a couple people in their mom's basement doing it, but, you know, if they find that vulnerability, you know, we've got to be able to work together to get everything back up and running.

RAVICH: It is a key responsibility of our government to serve its populace, for sure.

I'm going to bring in the rest of the panel. And first I'm going to turn to Mark Harvey.

You know, Mark, continuity of the economy is a tough concept to understand. So what kind of events would actually necessitate COTE?

It's a bit difficult to precisely pin down, so I just want you to do a bit more stage-setting by giving us a quick historical review of what happened after Hurricane Maria hit Puerto Rico in 2017 and how having a COTE plan might have helped in the scenario?

HARVEY: Absolutely. Well, I, very simply, Puerto Rico overnight went from living in the 21st Century to living in the 18th Century. And if you think of the economy as that motion and movement of capital through various markets, basically all of those gears ground to a halt. And that's really what we're talking about with continuity of the economy, is how to get that movement back up and running again so that capital can flow.

With Puerto Rico, it exceeded our capacity as a nation, with existing doctrine, to be able to handle that. And we saw these interdependencies, where the first thing that really challenged us in a big way, because we've got plans to get, you know, communications back up and running and transportation going again and the power grid back up. And in Puerto Rico, all of those intersected with each other. And so they had to be sequenced and worked together. We had to rebuild roads in order to get the crews out to the cell towers to get them back up and running, in order to help communicate where we can get the power grid up and running.

So it wasn't like they could operate independently. They had to work together. And then we started to see innovation in the middle of that. Really, with COTE, what we're talking about is something like what happens in government with continuity of government. Every individual agency has its continuity plan, but there's also a continuity of government plan that talks about how they all work together.

And in Puerto Rico we saw that providers restoring the cell service there agreed to repair each other's equipment. So instead of having to get an AT&T, Verizon and T-Mobile person out to every single tower, you could have one person on a tower taking care of three people's infrastructure and work three times as fast that way.

So that happens there. We also saw cascading impacts across industries. There's a lot of pharmaceutical and biomedical device manufacturing on Puerto Rico. So, because they were down there, all of a sudden, surgeries are getting rescheduled on the mainland and the sector impacts start to really cascade pretty quickly. And that's just on a small island of Puerto Rico. Think about, you know, a similar sort of event or something even more serious happening on Long Island, in the congressman's district there. You know, he's got two bits of infrastructure that carry a couple trillion dollars of transactions every single day, that provide our primary interface to Europe and much of the rest of the world.

And so if you've got those things down, all of a sudden, you know, losing $3 trillion of transactions in a day grinds a lot of the economy to a halt, and that's why we've got to have these plans that address interdependencies, how we leverage multiple authorities at the same time, and how our private industries are going to work together in a common capacity and not just in the interest of their own organization.

RAVICH: That's great, thank you. Tom, you know, Representative Garbarino was really talking about the necessity to kind of push the federal government to work closer and better with the private sector. And we often talked, when we served together on the Cyberspace Solarium Commission, about how forward thinking the drafters of the legislation were to make sure that there were private sector voices on the commission.

So what's your sense of the concerns around public-private collaboration on Continuity of the Economy? And what really — what is the proper role of the private sector in preparedness efforts for a significant economic disruption?

FANNING: Yeah, Samantha, thank you. We intentionally stayed away from words like "cooperate" and used words like "collaborate" in the Solarium Report. You just won't see "cooperate" very much. The federal government does not know how to operate private sector critical infrastructure. I'll stop.

I can tell you we've drilled this in the electricity sector several times over the Obama administration, Trump, and Biden. I remember there was one significant time where Tom Bossert from the National Security Council — terrific guy — invoked the FAST [Fixing America's Surface Transportation] Act, which gave the President the authority to operate the electricity system. He does that, and we turned to him and said "OK, what are you going to do?" And he had no clue. And he's a terrific guy.

Another time we were drilling in this was to evaluate a problem between an international issue. Toronto to New York City goes black, how do we manage all that? And the government came up with pre-written instructions on what to do operationally. They were garbage.

Every event is different. The government doesn't operate the complexity of a nationwide electricity grid, less so a financial system, less so communication networks. They absolutely must have the collaboration of the private sector in order to get America back on its feet from that bad day.

And I can tell you that, as I led the electricity sector now for — almost 10 years ago, one of the very first things I learned was that I can't think about electricity in a silo. We created something called the Tri-Sector Group, which included a collaboration of finance, telecom, and electricity, and those folks have continued to work at — first in a policy aiding session. They helped me on Solarium, they helped review legislation, and now they're actually playing a great role in evaluating how we operationalize the ideas that you and I worked on.

It is absolutely clear to me that we've got to have a situation — and I think CISA, through the JCDC [Joint Cyber Defense Collaborative], and even the NRMC [National Risk Management Center] will support the idea of collaboration between the federal government and the private sector. Without that, we will fail.

RAVICH: First, let — also, I just want to — if — you know, let the audience know isn't it wonderful and refreshing to have folks like, you know, Congressman Garbarino and Tom Fanning literally, like, speaking very clearly and plainly with passion about these issues?

And — you know, and that leads us to the question that we're going to throw to Mark Montgomery, who also pretty much never minces his words. Mark, you and Mark Harvey co-authored a memo that offers more than a discussion of challenges, but instead numerous specific recommendations to address the challenge.

And what's the difference between your memo and the administration's report? And why do you think the administration was so restrained?

MONTGOMERY: Thank you, Samantha, and I first want to thank Representative Garbarino for his persistent letters to CISA. I'm not 100 percent sure we would have gotten this report eight months late without him.

Look, there are some fundamental — I say four fundamental differences between the report we got from the administration and the report we wrote, which is I think the report that CISA wished they had written.

The first is the importance of the private sector. Look, the private sector is not just about sharing information. We have to treat them as people who are critical to executing courses of actions, and therefore making those decisions. And I think the administration report completely misses the opportunity to emphasize the importance of the private sector.

The second is, in the administration's report, there's a mistaken belief that today's governance structure is helping us prepare and mitigate the effects of a catastrophic casualty. They're not. We need to be more focused in the — our efforts, we need to — we need to make sure people are accountable, and then we need to make sure the private sector is integrated again. So those are the first two.

The third flaw in the administration's report, I think one we address a little more sharply, is a belief that the current emergency plans can cover Continuity of the Economy. They won't. They are very good plans for public health and safety, and that's important for a natural disaster, but as Mark Harvey said, they are not ready, you know, for that kind of loss of the northeast power grid kind of event. And I think Tom mentioned that the plans he saw were garbage, when you really start to take a look at that.

And I — I'd give you a fourth one — it's a lack of sense of urgency. You know, I think Representative Garbarino has put it in his letters, Tom has mentioned it, our— Mark's and my memo says it. We need to have a sense of urgency about this.

The vulnerabilities are increasing, the adversaries are becoming more aggressive, and we're treading water. And that — you know, really, I don't think CISA —I agree with Representative Garbarino, I think CISA's report, had they been able to write it on their own, would have been much different.

I think the processes of an interagency review and a White House involvement, the kind that says "hey, we're a bunch of pros" — and this is kind of a bipartisan affliction. It hits every administration. "We're a bunch of pros, we'll handle this problem when it comes." Well, that flies in the face of experience, right?

And the last thing I want to say is the Biden administration didn't create this problem, but after 30 months, they need to understand they own it. And I think a more aggressive plan that would have addressed those kind of four big thoughts would have really helped us, helped our national security, helped our economic continuity, and helped our country.

FANNING: Hey, Mark, can I jump...

RAVICH: Please, Tom.

FANNING: It— let me emphasize something else you said, and that is I have heard that people say "oh, well we have the power to convene." If you could imagine a disaster that's afflicting America, the lights are out, financial systems don't work, we can't talk, or whatever the problem is, now is not the time to be calling your buddies and try and figure it out.

We have to create an architecture so that there is an expectation of a shared accountability between the government and the private sector, and we have to drill that accountability so, in the event of a disaster, we're not making it up as we go.

RAVICH: Absolutely. So back to you, Congressman, you know, as Chair of — Chairman of the House Homeland Security's Cyber and Critical Infrastructure Subcommittee, you received a copy of the administration's COTE plan, or rather their response to the congressional directive to come up with a plan. So the report says things like having a COTE plan could “cause confusion," quote, or be “duplicative." They said they've got it all under control.

Mark and Tom doesn't sound like they're convinced. Are you convinced? Did the report actually assuage you that the federal government has it under control?

GARBARINO: Look, I yeah, I I've been focused on making sure thing — you know, government regulations and things aren't duplicative. You know, that's been a big focus of mine because we want people in the private sector, their cyber employees, cybersecurity employees, actually working on cybersecurity and not government regulation. So I get that, I get where they're coming from.

Under control though? I look, I don't know how have it under control. I mean, just —if there was a cyberattack tomorrow where six critical infrastructure sectors went down, I can't tell you who's in charge. Like, I couldn't tell you.

I mean, who —who's the — who is the key person on the government sector, on the government end, who is the key person of those sectors on the private sector end? I mean, I— there — it — there doesn't seem to be a structure there.

And I think in your report, in the letter you all did, you said we — there needs to — we need to set up a governance structure, a better one, for COTE. I think that's a great — like, there has to be a — if an emergency happens tomorrow, who's talking to each other? Who's making sure that the private sector and the public sector are on the same page?

I can't see how they can have it under control because it's not — they're not just going to hit one sector, it's going to be a couple. I mean, if this is an actual attack, they're going to hit several sectors at the same time. And it's not just — there has to be talk in between each other. I mean, as Mark was saying before and Tom was saying, like, they have to be talking to each other.

So I don't think they have it under control and — which means we're going to have to keep up oversight. I mean...

(CROSSTALK)

GARBARINO:... they've ignored our request, they gave — sent this report. They just didn't want to do it, it sounds like, and so we've just got to step up the oversight.

FANNING: Well, hey,— Chairman, let me add to this. I wouldn't put all this on CISA...

GARBARINO: Oh, no.

FANNING: ... this is really coming out of the — in — broadly written, the administration.

The other thing is they could hit one sector, but we are so interconnected as an economy. Even taking the electricity grid down has enormous impacts on communications, on financial systems, on healthcare. So, you have to understand the first, second, and third derivatives of the problem.

RAVICH: Yep.

(CROSSTALK)

GARBARINO: ... one hit on the sector — financial services sector, you know, you've got retail banking, which would affect the everyday person, but then we — you had those — like you said, the lines that are doing $3 trillion in transaction — I mean, these are all different — the sectors who make energy. You know, you've got nuclear, you've got natural gas, and you've got the grid. I mean, it's many — you're right, the — if it's — if it — if they do just hit one sector, it's going to affect others.

RAVICH: Yeah. So Mark Montgomery, you know, clearly the conversation — you know, we focused on why we need COTE, the importance of it, the failure of the administration's report to actually do it, but in your memo with Mark Harvey, you spend a good bit of time on trying to get towards answers on the governance' issue, focusing on what you call a national COTE coordinator and an industry COTE coordinator, a national COTE manager. Why are these roles important?

MONTGOMERY: I think this is really about — just like Representative Garbarino and Tom have been alluding to, it's about governance. And it's not any single individual's going to solve the problem but it's about having the right structure in place.

And you remember our good friend, yours and mine and Tom's, Senator Angus King, the chairman of our commission, he used to say repeatedly that structure is policy and you need to have good governance structure if you're going to have a good governance policy — you know, for, in this case, cyber resilience and recovery.

The key to this is having someone in charge at the White House. I'm— I understand that's necessary. If you want — right now, I think it naturally falls on the Homeland Security Advisor. But that person is purely an interface between the process and the President. Their staff of five or six people is not going to be able to govern this.

And they're top cover on hard decisions, you know, it — when you're trying to make budgetary decisions ahead of time, having someone in the White House who's responsible is useful. What you really need are the next two people, you need a — two organizations.

You need a day-to-day process executor for this. You need someone who is going to an organization that's going to keep agencies focused on the issue. You need to keep an integrated effort moving along and you need an interface with the private sector.

And that's where I think the White House intervened and killed this idea, because other agencies don't like to say CISA's in charge or the Department of Homeland Security's in charge. And that is a flaw that we have in our system, and it's bipartisan, it existed in the last administration, probably existed in the Obama administration. At some point, someone needs to be in charge ahead — left of boom, left of the event, so they can do the planning, the processing, the exercising.

The final thing I'll say is you have to have private sector leadership. You know, it has to come from energy, financial services, transportation, communications, IT, water. We've mentioned them all. They have the expertise. They own 85 percent of it — they operate 85 percent of it. They know how to do — they need to be critical to that preparation, that exercising, and the decision-making about how you restore it.

So if you have that national COTE manager, probably someone the Secretary of Homeland Security designates, and national — and sector COTE liaisons, your one senior — probably former CEO of a major company that then leads others, and the — and you can naturally draw on the sector coordinating councils for this leadership — and these people need to be in a position that when a real crisis happens, they're inside the tent, clearance wise, access wise, classification wise.

We used to — in — back in the days of the Cold War with the Soviet Union in the 1950s, we had national reserve, you know, senior executives, you know, where we could bring them, co-opt them into the government very quickly if that was necessary for decision-making.

There's a lot of opportunity here. I'm not arguing for any specific role there, but what I'm saying is you need these three broad things — top cover at the White House, someone in charge, and then a private sector leadership structure — to match that national COTE manager.

RAVICH: OK, so let's — let — Tom, I hear, you know, Mark talking about — and it's written in the report — about an industry COTE liaison. And of course, I have to get, you know, your thoughts on this.

Is it needed? What kind of person could serve in this role? Maybe one of the pictures that is currently on your screen would be the absolute perfect archetype of such person — OK — but not putting you on the spot for that. But the — generally though, you know, what is needed for COTE in a coordination with the owners and operators of the relevant infrastructure, along with the government in all levels? I mean — cause you've got to assess the damage, prioritize restoration efforts, right, rally necessary resources, ensure national needs are met. I mean, you know, what are your thoughts? Can it be done?

FANNING: You — are you asking me?

RAVICH: Yeah.

FANNING: Yeah, Samantha, we spent a lot of time and we — I think we failed on the acronym marketing business, but we came up with what we called SICI. That's S-I-C-I, Systemically Important Critical Infrastructure.

When you are — and we do this in our industry and I'm sure every other industry — when there is a — from an electricity standpoint, when there is a major hurricane, one of the things that we have to have immediately is a sense of priority, a triage plan, if you will, that will work with the most important things first, get them back up, and then as a consequence, get everything else back up. So this idea of SICI identifies, before the problem happens, where the most important critical infrastructure resides, OK?

Taking a step down from that is the idea that CISA has put forward, which is still also a good idea, and that's SIE — systemically important entities. So these would be the companies that own the critical infrastructure. And what you would do is work together. So when electricity joined finance in its ARC [Analysis & Resilience Center for Systemic Risk], one of the things we did was understand in a very robust, deep way how we work together and how, when things go bad, they come back up. That manifests itself as a risk register that we would use during a time of calamity to set as a priority, what should our actions start to follow? That's a very dicey issue. It should be absolutely classified at the highest levels of government, and the federal government needs to understand that is how we're going to approach the problem. Every problem is different, and therefore, every application of these concepts of priority and triage may be different. But at least you start down the road, you build muscle memory, and you're able to effectuate a plan.

Let me give you an example of good work that is currently going on inside CISA, say, at the JCDC. It does three things. This is the joint collaborative environment. The intelligence community, sector-specific agencies, private sector, and those will hold the bad guys accountable: DOD, FBI, Secret Service, U.S. Cyber Command.

The first thing we do is evaluate the battlefield in as much real time as possible. Southern Company gets attacked about three million times a day, so that's just one company in one industry. What is the whole quilt? What is the fabric of the attack surface and the attack vectors coming in look like? Understand that.

Two: As you see these attacks form and develop, pre-boom, let's start doing things to harden the attack surfaces, and if we have a problem, get back on our feet quicker.

Three, is really post-boom: Let's have an integrated response.

Now, I gave you a simple example of something we're doing inside CISA at the JCDC. This needs to be done comprehensively across the United States government. There's ways to do it. Having a single person work with the private sector to recruit captains of industry, if you will, by sector makes a lot of sense.

And then to the concept of the COTE manager that Mark mentioned, I think you can leverage entities like the Tri-Sector Group. These are operational-level people, not CEO people, that can start to surface the issues and get CEOs to deal with them.

RAVICH: Absolutely. Absolutely, and I'm going to pause you there for a moment just because we're going to lose Congressman Garbarino in a moment or two to go do the people's business.

But I do have a question here from Eric Geller at The Messenger before you have to leave, Congressman. He asks, "Representative Garbarino, what can you tell us about how your subcommittee will press the administration on COTE?"

GARBARINO: Look, we — I mean, we just got the report a couple weeks ago. I won't even say "plan", because it's not a plan. We're going to continue with oversight. We — and we're — and I'm — it's not just going to be my subcommittee because it's not just — you know, these sectors don't just fall under my subcommittee. I'm going to work with Chairman Gallagher, work with Energy and Commerce, work with Financial Services. We're not — you know, I'm — Gallagher and I took the lead on this. We're not happy with what — at least, I — you know, I don't want to speak for Congressman Gallagher, but I'm not happy with what came out, and I can't imagine other people are, either. So we're going to continue with our oversight and continue up the pre- — continue on the pressure — continue the pressure on the administration to make sure that they follow congressional directive and just don't thumb its nose at it.

I mean, it's scary. Like I said before, the fact that we have these nation-states, these — and these criminal actors both from within and without the country with the ability to just shut down our economy in certain sectors, it's scary. And every day we wait to come up with an actual plan is one day closer to disaster.

So — and when something actually happens — and we see — all see what happened after Colonial Pipeline. That was barely anything. You know, this is —that's —it's a drop in the bucket compared to what this could be, and people freaked out. So you know, we're going to — it's not just going to be my subcommittee. We're going to stick with it because we do over- —we do have oversight over CISA. Homeland has oversight over other sector risk management agencies as well, so there's going to be oversight continuing from our committee, but there are other committees that are going to join in as well, I think. But you know, we're going to do our job. We're going to continue to push the administration to do its job.

RAVICH: Well, thank you. Thank you so much and thank you for attending this.

GARBARINO: Thank you very much. I was great. I'll see you all very soon.

RAVICH: Absolutely, absolutely.

OK, before we turn to Q&A, I'm going to take the moderator's prerogative and ask one question to Mark Harvey.

So just to hit home on a couple points, your paper talks about making sure that certain private sector players can participate in COTE implementation, presidential decision-making by using something called the National Defense Executive Reserve Corps. So I worked in the White House for five and a half years, and I'm not sure what that is or how it works and — but I guess this just demonstrates that the authorities who may — we may need to use in a COTE scenario may be not well-understood or practiced. How do we make sure, and how do we know that the authorities aren't trying to just figure this all out in the middle of the crisis, like what Tom was talking about? So talk a bit about the role of exercises and a national COTE exercise specifically.

HARVEY: Absolutely. I'm — you hit the nail on the head there, is that there's so much in the mix for COTE. There's so many things that we can draw on, and if anybody tells you, "Hey, we've got it under control," then the immediate next thing is to say, "OK, show me. So show me an exercise to how you're going to leverage this prioritization that we were just talking about. How are you going to get it done when you've got the" — apologies of the alphabet soup here — the NCIPP [National Critical Infrastructure Prioritization Program], Section 9 list, level I/level II lists, systemically-important financial market utilities, G-SIBs [Global Systemically Important Banks] — all of these other rubrics that exist out there. Great, they operate fundamentally good work from a day-to-day basis. But now in this complex event, they're all going to clash. “So show me that you can actually work through that. Show me that you can leverage the actual authorities that we have across the federal government to be able to execute. And as Tom was saying earlier, that we can actually order something that can be executed, right? We can't do that without having the appropriate private-sector voice in the room to be able to help with that prioritization, direct that action.

And today, when we've got all of those things available to us but no plan on how to pull them together, it's like me saying I've got, you know, flour, sugar, eggs and milk in my pantry. But am I making pancakes or am I making waffles or cookies? It's all going to go together some different way. So we need the recipe, right? That's what that plan is about. And that recipe is going to say "Here are unique authorities that we haven't used in a very long time but are still on the books."

Just like Mark was saying earlier, go back to the '50s and that Cold War planning, when we had private-sector mobilization, and how we would actually leverage some of these key industries. And we were investing together with private industry to talk about bringing a national approach, not a whole-of-government but a whole-of-nation, everybody working together, inclusive of public and private, on how we execute. That's what our exercises for this need to be.

So we need very clear objectives on executing that governance, performing the prioritization, leveraging very little-understood authorities, to make sure that were not running into these roadblocks right in the middle of it. Just like any good emergency manager knows, you don't trade business cards on the site of a disaster. You do it ahead of time, in the no-fault learning environment and run into these issues in a good regular exercise that, by the way, the private sector needs to be right in the room during the planning stages of so they can really inform and stress ourselves hard.

RAVICH: Right.

HARVEY: Let's, you know, figure out how to break this now before it's really violently hit.

RAVICH: Well put. Well put.

You know, Tom, we have a question from the audience about, you know, another thing that may be woefully out of date, which is Presidential Policy Directive 21. For those in the audience, it states — quote, it "establishes governance for critical infrastructure and security with the private sector."

So the Obama administration issued PPD 21 in February — wait for it — of 2013. So it seems like it could be egregiously out of date. Ten years, I'm sure, in your industry, is quite a long time. Things change. The sector-specific plans, also, that enable the National Infrastructure Protection Plan are also eight years old. And many are just cookie-cutter copies of others, rather than a thoughtful exploration of sector-specific risks and recommendations.

So, Tom, I assume — I assume a lot has changed in your industry over the last decade. People are — yeah, it would seem? But correct me if I'm wrong.

(LAUGHTER)

FANNING: No. In fact, these plans need to be written with the old Wayne Gretzky idea, "Skate to where the puck will be." Thinking about where we were 10 years ago, and you think about, now, the advent of artificial intelligence, perhaps even quantum computing, smart grids, the whole thing, it absolutely is a different ball game. I'm sure that's true for every industry.

RAVICH: Yeah. So Mark Montgomery and then Mark Harvey, you know, comment on that as well — if you choose. I mean, the National Infrastructure Protection Plan has not been updated since 2015. Why is that important?

MONTGOMERY: So the— I think this is all leverage on the — what you mentioned first, Presidential Policy Directive 21. And for — you know, it is, like you said, 10 years late. I think this administration, at the very beginning, understood they needed to rewrite it, but 30, you know, plus months into it, we haven't had anything done.

The really egregious thing is that I think the National Infrastructure Protection Plan and the sector-specific plans have been rewritten, and I think they're being held for the most part — and maybe not, you know, the final, you know, "t"s haven't been crossed and "i"s dotted, but they're ready to go, pending PPD 21 getting done.

So the White House's inability to get PPD 21 is really holding up the whole structure. And look, plans aren't everything but plans allow you know, it the value of the plan is the — working it with the — is taking it out and then exercising it with the private sector, assessing where it wasn't successful, retooling it and redoing it.

Not only should these plans be done now, they should be — they should have on them — they should be timestamped for 12, 18, or 24 months, depending on the sector and the national plan. And that's what's killing us, this lack — we're treating an emerging technology issue like a — a World War II — you know, a Cold War bureaucracy.

We absolutely need to get the PPD 21 done, we need to get the NIPP (and the National Infrastructure Protection Plan, sector-specific plans — and frankly, I would detach them from PPD 21 at this point. I would get them out there so they can be put through their paces. They're better than the cut and paste versions they're replacing.

I know that. And in fact, the way I know I'm right is DOD's exempted itself from its process, taken their own, you know, sector-specific plan, rewritten it and kept it in a draft form, unapproved but being executed by them. And that's all you need to know, is when the Department of Defense takes off in their own direction, it's cause they've gotten tired of the rest of the federal government.

So, you know, from my point of view, absolutely this is one of the job one priorities.

FANNING: I would — hey — hey...

(CROSSTALK)

RAVICH: ... please, Tom, go ahead.

FANNING: Yeah, if I could jump in here. Son of a gun, I think one of the biggest ideas coming out of Solarium was the reimagination of national security, which requires, as an accountability to the private sector, for the private sector to collaborate with government. How can you rewrite PPD 21 and all this other stuff without having the private sector work with it?

It's being done independently in government. I think they talked to sector-specific agencies and all of that but we don't have, I think, a real collaboration, a real operationalization of this new reality, this reimagination of what is national security.

It must require the private sector to collaborate.

RAVICH: Yep. So I have a question for

HARVEY: You hit the nail on the head there.

RAVICH: ... oh sorry Mark go.

HARVEY: I was on the writing team for the National Infrastructure Protection Plan back 2004, 2005. It's fundamentally two things — the risk management framework and the sector partnership model, and those are proven, they're working.

What we have here are challenges with new and emerging technology and our interdependencies. And we knew right when we got the first one done in 2005, we ran headlong into interdependency problem set and just haven't solved it, and said "oh, that's hard. We'll go build more lists in the meantime."

Instead of tackling the hard problem, we need to tackle the hard interdependency problem, whether that's policy, whether that's plans. At the end of the day, Tom just nailed it, it's got to be operationalized.

RAVICH: Yeah. And before I get to a question for Tom from Sara Friedman of Inside Cybersecurity, I mean, I can, you know, just think 2013 or even 2015, when someone mentioned cloud, we all still looked up, right? I mean, the idea our entire life, all our businesses reside in cloud computing, and that isn't really considered in — you know, from 2013 plans or 2015 plans. It just kind of — really kind of underscores how time has moved on and the plans to deal with Continuity of the Economy and the fundamental documents have not.

So — but Tom, you know, is there a role for the CISA Cybersecurity Advisory Committee, upon, you know, which you sit and potentially chair, to help the government with the COTE planning?

FANNING: Oh, of course. You know — but let's be clear, the COTE plan operationalized isn't a CISA thing, I think it's a whole-of-government thing. You know, it's going to require FEMA [Federal Emergency Management Agency], it's going to require all of the sector risk management agencies.

Absolutely, CISA has a role. For example, in the National Risk Management Center, sector by sector, what we do is create these risk registers and analyze interdependencies. And I can tell you the work that electricity collaborated with finance — we uncovered things we didn't know.

For example, evaluating this first, second, third degree of derivatives of supply chain risks. Oh man, all of a sudden, we found there were five elements of the supply chain to the nation's backbone transmission system that could potentially be at risk. We found that out two years ago, and now we're taking steps to deal with it.

That kind of hard, ground level work is starting to happen, it needs to mature. I think CISA's doing the right thing. CISA can't carry the ball here. This needs to be a whole-of-administration approach.

MONTGOMERY: And Samantha, if I could bring up one thing on something you just said — I — one of the worries I have on PPD 21 is that there's going to become a sense of urgency at some point to get it done. Historically, what that means is something gets trimmed heavily, all challenging issues dropped.

And you brought up a great one — cloud — or the cloud computing. You know, it was our strongest recommendation in a number of papers that cloud computing is a critical infrastructure, and if we don't see that come out in PPD 21, I'm afraid PPD 21 is on its face a failure.

And so we need to keep the pressure on the administration, not just to deliver PPD 21 but to deliver a PPD 21 that's properly updated for the environment we're living in, and that means cloud computing, and for the same reasons, space infrastructure, space support infrastructure.

We need to have some additional new critical infrastructures. You may be able to drop some, combine some, but if you don't add cloud computing, add space systems support, we're going to have a real problem.

RAVICH: So I want this conversation to really continue but I've been told that it has to end at — in a few minutes. But I want to kind of wrap this up by saying that, you know, two days ago was the 22nd anniversary of 9/11. I kind of can't even believe it's that long.

Anyway, we felt then that the unthinkable had happened. And we have spent the next two decades making our country stronger and more resilient for a wide range of attacks, and yet as we heard today, our government is being remiss in not creating and exercising a plan for Continuity of the Economy.

And such planning is hard but that is absolutely no excuse. And the visions of leaders like Congressman Garbarino and Tom Fanning, alongside of the important research and analysis of Mark Harvey and Mark Montgomery, will help us become more secure and will help the government march down that road to making the citizenry more secure in this critical issue. So we hope the government watch this event and those that can do something read the report and follow it.

And with that, I thank you and I thank all of the panelists.