This transcript is made possible through the sponsorship of JobsOhio.

Maj. Gen. Anthony Genatempo:

All right. Good afternoon ladies and gentlemen. That was absolutely weak from the hundreds of faceless, hopefully smiling people in the audience today. Good afternoon everybody. Outstanding. I am very excited to be here today to moderate this panel of experts in their field. And one of our advertisements we just saw was a great lead in for, what exactly are we doing in the realm of cyber technology? And the word we're going to be using today is cyber resiliency. My name is Major General Augie Genatempo, and I'm the program executive officer up at Hanscom Air Force Base for our C3i and networks directory. A large part of my portfolio exists down in San Antonio, working right next to the 16th Air Force, providing capabilities to that incredible mission set. And we're going to talk a little bit about that today. So, let me set the stage for all of us a little bit.

Information technology, operational technology, weapon systems are all dependent upon the cyber domain, more so now than ever before. And our ability to generate air power and ensure peace depends on the confidentiality, integrity, availability of our data in this domain. Now for a long time, we've protected it simply by using perimeter security controls. Every Airman is responsible for cyber security. But right now, we know better than ever, that our near peer threats and our adversaries are not just going to be kept out from perimeter controls. So what are we doing to say once our adversaries have penetrated our system, how do we still ensure mission success when that happens? And that's where resiliency comes in. And the point that we are going to hopefully be making and to getting everybody on board with this movement, is that we need to ensure resiliency is baked into every system that we procure.

That starts at the very beginning. For too long, as a program executive, as a program manager, cyber resiliency, or cyber security, was the add-on after development. It was the thing we had to correspond to, but we had to come up with our full design first. And more often than not, we did not accommodate for the threat that was out there, the evolving threat that was out there because we're talking about years of development things change over years. But if I have to take care of cyber security after my design is complete, I am pretty much out of money and out of time at that point.

So one of the other main points that we're going to make today is how do we move that back into the beginning of the development process using the models that the development team is using and having the cyber experts as part of the development team? So today, I have three members from industry that are absolutely experts in their field. And what I'd like to do is have each of them briefly introduce themselves, tell you a little bit about where they're from, and then I have a couple of questions to pose to them to get after some of these topics for you. So I'd like to start with my immediate left here. Tom, go ahead.

Thomas P. Michelli:

Hi, my name's Tom Michelli. I'm with Leidos. I'm a strategic account executive for cyber across all of our operating groups. Before that, I spent 17 years in government. My last job was on the joint staff. I was Vice Director J6, command control, computers, communications and cyber. And before that, I was acting deputy CIO for cybersecurity and CISO for the Department of Defense, had the opportunity to be CIO for immigrations and custom enforcement, US Coast Guard, and back in the day, I did offensive and defensive cyber as a Virginia National Guardsman deployed for OAF102.

Maj. Gen. Anthony Genatempo:

Outstanding. Ma'am.

Latisha R. Rourke:

Hi, my name's Tish Rourke and I'm the vice president for cyber and intelligence for Lockheed Martin. My career, I've done everything from anti-submarine warfare, mine warfare, electronic warfare, and now I'm involved in the cyber and intelligence industry. So it's just been a great growth experience and I'm really excited to be here and talk to you about cyber and resiliency and the challenges that we have.

Quinn Bottum:

My name's Quinn Bottum. I'm one of the founders of a company called Swoop. I do not have the distinguished pedigree of these two, but I started Swoop 10 years ago. I was doing it while I was in college, I was doing an undergrad in Chinese computational cybersecurity in applied math. I finished my graduate thesis on Chinese exploitation of power management systems and decided to start a company around some of the software that we were using. And somehow, 10 years have flown by, and I'm getting to work with these two now. I'll give it back over to you, Augie.

Maj. Gen. Anthony Genatempo:

All right, thanks very much. So, all right, the first question I have is to Tom. And Tom, what I'd like to do is for you to share your thoughts on what you think we as a department of defense should be doing to increase the speed and scale of adopting of greenfield technologies while ensuring cyber resiliency? And then conversely, what do you think the biggest challenge is for our systems that are already fielded to make them more resilient?

Thomas P. Michelli:

So whatever cyber conference you go to, the first thing they talk about is people. And we have a talent shortage, and it's not just the programmers or the computer geeks or the cyber geeks, it's everybody in the ecosystem. And as General mentioned, we're talking about resiliency now, too. So resiliency is not just your system, it's fighting hurt with your partners on the left and right, and downstream and upstream. So when I talk about people, we definitely need to improve the STEM research, the STEM capabilities of everybody in our nation, assess them into the military or contractors or academia to help us with this problem. But it's also the mission owners, it's the contracting officers, it's the CFOs. General Hyten, when he was commander of STRATCOM, talked about bowling the frog. You have risk management. And when you have the frog in there and you take a risk in not putting in some cyber security, not taking the time to design in cyber security in the system, you take a little bit of risk.

Well that's one part of the system. Let's say it's the satellite in the air. The ground system, they take a little bit of risk. Well, the satellite, the hardware in the sky, relied on the ground system. Well, they don't realize they're both taking risk. So the risk all of a sudden becomes compounded, the heat goes up. The contracting officer, they're folks like Leidos, Lockheed Martin, and others, are interested in internal research and development to help mitigate some issues, to bring things to speed. Competition with China and Russia, bring that to bear. But the contracting officer doesn't know how to enable the requirer or the PEO or the PMO, to go out and work with industry to accelerate that. So it's building a culture across the high schoolers, the college folks, the Airmen, the Guardians, the contractors, on how we bring this all together to provide design in the system, the resiliency of cyber security we need.

The other pieces back to the dollars. The first thing is, well, we want more functionality. We want the whammo dying capability in our system, but we cut back on transport. Transport being how we communicate to other systems or the user. A lot of times, we want backup, but that's the first thing to go. So as soon as we lose transport communications, the system's useless. So we need to educate the whole ecosystem on deploying that greenfield. On the brownfields, it's the same thing. It's getting us, as

a nation, and our allies and partners. I see some allies and partners are here. We're not going to fight alone. So how do we ensure that capability of cyber secure across all our allies and partners, ourselves?

Maj. Gen. Anthony Genatempo:

Outstanding. Any other comments?

Latisha R. Rourke:

Sure. I would like to say, you're exactly right, Tom. Hey, design it in. But what's more important is making sure that we test, we continually test and we share those solutions and those failures with other systems and platforms. It's not just, "Hey, it works in my system," or, "It's defensive against my system." It's, "How do I share those lessons across multiple platforms and sensors?" So ensuring that, from a cyber, we talk about the defense industrial base sharing those cyber attacks to protect each other. We've got to do that across platforms and sensors.

Quinn Bottum:

I think the only thing I'd add to it is that maybe at a less strategic and more operational level, is we field these things and we try to exchange lessons learned and how something might defend against one vector of attack on one given system. It really becomes a matter of how do you get ahead of the off the offense? Because as much as lessons being shared helps, you also need to be able to do it in the moment. If I'm the attacker and I go after a system and given defense works, that informs my next attack. But in a lot of the times, the defensive systems out there, that system then stops until maybe an after action report or a war gaming when that comes out. And so the next defensive system that needs to know about that, the previous attack, has no idea. There's no information sharing. And so the attacker is constantly at an advantage that compounds over time against the defense. And so it's got to work across multiple different time horizons for us to really get an impact.

Thomas P. Michelli:

Can I expand on it? Exactly right. Another thing is when I first got started in this back at OAF102, we red team things and we would say, "Drop the mic, you're all messed up and walk away." The defenders then, would try to mitigate what we found. And it would be this two instances where, if the offensive was working with the defensive, we could train the defenders on where we're coming from. And the defenders will say, "Hey, you didn't get this because this is what we were thinking. And oh, by the way, we were more worried about this."

So we need to do the red and blue team. We need a purple team. And that's all the way from requirements to design to fielding. And when we field, we need to work with the mission owner to say, "Hey, with all the cyber security built in and the resiliency, there's still going to be times we're going to fight hurt. So what are you going to do with your CONOPS?" And I think you brought this up before, "How are you going to fight hurt? With all the stuff that we've put into this, all the risks we've known we've taken because there is restrictions on money and capability. How are you going to fight?" So we need to purple things up.

Maj. Gen. Anthony Genatempo:

And some of you may be asking out there, "Well that sounds like an awesome idea, Augie. What are you doing to get after that?" Well, the answer is we are. Your acquisition community is getting after that and especially for the newer systems and platforms that we are bringing online. So some experience that I've recently had, my job previous to this one, I worked in the nuclear weapon center and I was the program

executive for strategic systems. So working on our ICBM replacement, the Sentinel program. A lot of the acquisition forums that you may or may not sit in, you hear a lot about digital transformation, you hear a lot about model-based system engineering, hear a lot about digital twin. What we found in Sentinel is that an extraordinary amount of time was being taken up by the safety community, the cybersecurity community, and my very own nuclear certification community.

By waiting for the design of the system to get to a certain point, then each of these communities would create their own model of the system to apply their own controls, which took an inordinate amount of time and money and manpower, and then feed that back. Getting to the point that I mentioned before, at a point where I as the program manager, have run out of time and money to do anything. So, the Sentinel program as incorporated, is basically a unified theory of certification and safety. Nuclear certification and cybersecurity are using the digital twin model that the developers are using. They are running their controls, they are running their tests, they are running their red teaming against the design at the time and then feed that back. And then, when the design changes, they are right there to do that again. So the iterative process that we are going through is ensuring that when I get to the end of the engineering, manufacturing, and development program, I don't have this big gotcha going, "You are neither safe, nor nuclear certified, nor able to be connected to anything out on the AFNET."

And for something as large and as critical as Sentinel, not saying that the rest of it is not, but that program needs to be ready to go when it needs to be ready to go. And I can't have those tent poles be the long poles in the tent. So the red teaming aspect of it, Sentinel has brought that team in sitting right in the same sandbox computer model that we are running different design iterations on, making sure we don't go outside of any of the cyber security bounds. So thank you very much for that. Okay. Onto you, ma'am. From a larger extent, you and I had a conversation about this on Friday and the conversation we had, I think, would be of very interest to the team here. So what do you think the biggest challenge is that the DoD and our industry faces with the cybersecurity field and what should we be doing to face those challenges in a head-on fashion?

Latisha R. Rourke:

Sure. I believe our biggest challenge in the cyber arena is our workforce. For every job out there, for every 10 jobs out there, three of them are left unfilled. So number one, we've got to grow the talent in our cyber workforce. We've got to organically grow it. And how do we do that? We've got to start right at the K through 12 level, get students, all students, minority students, females, everybody interested in STEM. You saw in the public service announcement prior to the session, where industry is advocating for STEM, we've got to do more of that. One thing that we've talked about is, there's that old adage, if you teach a man to fish, he'll eat for a lifetime. Well, we've got to teach teachers about cyber because they are that force multiplier that can help us to encourage students in K through 12 to go into STEM and specifically, cyber.

And then secondly, we've got to, I'll look at all my industry partners that's in the room. We're doing a great job of poaching all of our employees. It's a vicious circle. Yeah, it's the truth. We're spending a lot of money recruiting talent, but what are we doing internally to encourage our employees to stay in cyber? Giving them challenging assignments. I'll look at the Air Force, I'll look at DoD and say, "Gee, a lot of what we do, our employees are working in skiffs." Well, we've just spent three years in COVID and the country went on and we learned how to work from home.

So maybe people that work in skiffs every day, three years ago and work every day now in skiffs, maybe we can figure out a way to say, "Hey, this part of your work isn't classified and so you can do this part of your work from home." How do you grow that workforce by saying, "This is unclassified. You can work from home." Because that is something that is causing people to leave this industry. They'd rather go

where they can work from home than stay in this industry. So we've got to encourage more students into STEM and we've got to keep the workforce that we have.

Maj. Gen. Anthony Genatempo:

Let's see. Any other thoughts folks?

Quinn Bottum:

So I think, building upon that, there's the notion, you never waste a crisis and there's no secret that we've had some leaks in the last number of years of exploits and different capabilities. I'm sure I'm going to get myself in trouble with every lawyer or policy person in the room. But if we're not going to waste that crisis, part of that STEM process is making it cool and jumping into it right away. So there's, let's call it the hacker community. There's this counterculture, rebellious type nature. I can guarantee you because we see them when we're recruiting and it becomes a clearance process problem, they're going and getting those tools on the dark web. They're going and downloading them. They're playing with them. They're, hopefully not happening, but probably using them from time to time.

So how do we create sandboxes at a high school level, at a collegiate level, where we're actually trying to harness that and take control of it a little bit and maybe guide it and steer it towards something good where, if they're trying to defend a system now and as part of a class project or part of some type of program. They have to now try to defend that system against something that's real, that's been out in the world and has actually had an effect.

Or if they're learning how to use that offensive capability, they have to apply it against many different systems and look at how different defenses respond to it so that they see it's not a one size fits all. And they actually start to bridge the gap of what they understand about worlds that typically only live in a skiff, but somehow have gotten out.

Thomas P. Michelli:

And I think the other thing, back to the greenfield. Getting everybody together from the imagination, the thought in the eye, all the way... Sorry. Thank you. The imagination all the way to the requirement design to fielding, it is getting together industry, the services, our allied partners, we've got a tech bridge now in the UK and I think we're expanding elsewhere, getting it all together and learning how we can make up the people gap with artificial intelligence, machine learning.

So for example, back to resiliency. When I was CIO with the Coast Guard, on the cutters, we had a switch. It was a manual switch. We had to have a person move the switch. ESPN, no ESPN. The bandwidth, if we needed the bandwidth for a mission as opposed to morale and welfare, somebody had to go flick the switch. Well, if we could automatically say, "Hey, we now have more mission requirements, we're going to cut off ESPN." That could be done automatically. Also, in the red teaming and blue teaming, the defense and offense, if we could incorporate artificial intelligence, machine learning into that process and have faith that it'll work ethically, that will help, as well. So again, it's using all of our national assets and our allies' assets, people and technology together.

Maj. Gen. Anthony Genatempo:

I'll expand a little bit on what Tish said, and I absolutely am not going to devolve into a conversation about telework and telework policy. What I will do is, as Tish mentioned, life did change and we did operate. And as we get back, what I have seen amongst some of my organizations that I've worked with, they're just hitting the easy button and say, "Okay, we went from 100% telework and then policies changed and morphed over time as the conditions changed in our local areas. And we went either to a

70% or a 60% or a 50% posture." And now, when we got to a point where there was an all clear in a large part of our country, all supervisors said, "Okay, everybody back to work full time."

I personally, don't believe that that's the way we're going to be able to go. People have had this experience, they have had this taste. And I will offer up the personal observation that people who never, ever expressed a desire to telework in their entire lives now like it a little bit, for a numerous number of reasons. And it gets directly to, are we going to be able to retain the people if our competitors, and by competitors I mean other industries that can capitalize on the expertise, the same expertise that we're looking for, are offering different things that people now like and are accustomed to?

And if we don't get on board being in front of that bow wave, I feel we're going to see more of a drain in the critical skills that we need. So what my ask is, what I'm asking my team, sitting right here in the front row, what I'm asking all of you is, don't hit the easy button. Try to come up with the solution set that incorporates what has happened to all of us into the path moving forward and let's see if that actually does help in our retention.

All right. Mr. Quinn, all the way down at the end, what I'd like to ask you about, and you're going to have to do a little bit of explaining for the group because you had to explain it to me. How do you think DoD and the industry should be changing its operations to get after the asymmetry between attackers and system operators to close the imagination gap? Now when you first used that word, I had visions of Mickey Mouse and Disneyland and that's not what you were referring to. So if you could expand on that a little bit for me, for the group, and then really dive into the essence of your position right here.

Quinn Bottum:

So imagination gap. I've touched on it a little bit in some of the other comments I've made. There's a fundamental asymmetry between how offensive operations work and defensive operations work for a lot of people that build defensive technologies. The reality is, is that the best of the offensive capabilities we hope are typically not widely known. They're not widely publicized. Hopefully they're highly classified. And so what that means is then there's this imagination gap where those that are building the systems to defend, they can't even imagine what an attacker might be able to do. They can't imagine that they might be able to jump from this air gap environment to another. They can't imagine that a clock could possibly be used nefariously against them. And that's not a knock, that's not a criticism. It doesn't make them less intelligent. It's just, it's such an opaque and ambiguous world that they can't imagine it.

So if you can't imagine it, then oftentimes, you can't build something to defend against it. And that's where we find ourselves, in my opinion, maybe incorrectly, we find ourselves fairly often. And it actually, then I think you see it happen in red teams or you see it maybe another asymmetry similar to it in how we do red teaming today. To be truly ready to be resilient, to be cyber resilient, to be able to fight through the inevitable compromises or system outages that are going to happen, you have to be tested against the best of the best and know how you're going to respond to it, where there is degradation. But to be tested against the best of the best, you have to be proven technology. To be proven technology, you have to be tested against the best of the best. And so we get into this constant do loop where you're going around and around and around and it's a chicken and an egg problem.

And what the impact of that is, you get a number of, you get reports that come out of penetration testing where there's statements like, it is vulnerable to X, or this could happen. And that's where the sentence stops. Even as you move into classified environments, that's where the sentence stops. And that does two things. The defense has no idea how to incrementally or iteratively actually start to maneuver or to revise their capabilities. So we don't get better and we don't take the lessons learned from project to project. But maybe even more critically, it means that we have situations where the

conditions, the operating environment, what comes before that potential vulnerability or after it and the impact and how far it could move or proliferate, that's missed.

And so when you give then, a commander that decision on how they want to bound the risk, how they want to manage that risk, there's a bunch of context that's missing and that's not decision quality data. So I think, as we look at red teaming, we have to find ways, and it's difficult because there's a reason why a lot of these capabilities are as classified as they are, but we have to find ways of being able to close that imagination gap, but then also, get into much more just nuanced red teaming that allows for a much better decision quality data and a much faster iterative loop on building better defensive systems.

Maj. Gen. Anthony Genatempo:

Outstanding. Any other thoughts? No other thoughts. All right. And I'm going to get to our last question, and this is for all of you. No matter how we look at cyber resiliency, I don't think any of us would disagree that there's always going to be a human in the loop. So with that said, I'd like to hear from each of you about how you think CONOPS should be changed to best utilize AI and machine learning cyber tools.

Thomas P. Michelli:

So, go back to Quinn's imagination, I think [inaudible 00:26:59]

Maj. Gen. Anthony Genatempo:

Microphone, microphone, microphone, microphone, microphone, microphone, microphone.

Thomas P. Michelli:

See, it was artificial intelligence if I looked at it, enough. The imagination thing, is just great. So how do you imagine incorporating all these great new technologies? And I know it's going to sound boring, but I keep going back to the same thing. And that is educating the whole ecosystem from the people we're going to be assessing, either in our country or our allies and partners, getting them thinking about all the cool, neat ways to do things, from the first initial idea of a requirement, getting the contracting officer, getting the financial people, getting the legal ethicists involved in what we're doing, the programmers, the cyber folks, the financial folks, so that we have a complete understanding of where we're heading and how we're going to build in the resiliency.

War gaming, red teaming, blue teaming, defending, supporting, and then also sustaining. We look at a weapon system, we talk about sustainment. Well, all our IT tools, all our cyber capabilities, our weapon system, we need to look how we're going to sustain, support, and fight that system hurt from the very beginning. And then, again, both in our nation and our allies and partners, we have folks who are doing internal research and development who would love to hear further, "Are we spending the money in the right place? Are we meeting your requirements? Will we fit into your CONOPS? Can we do this war game to get ahead with speed?" And we're all talking the same language.

Maj. Gen. Anthony Genatempo:

Outstanding. Tish?

Latisha R. Rourke:

Okay, I'll pick up from there, Tom. Thanks. Quinn said it, tom said it, the general said it. How do we get ahead already in this CONOPS? Instead of being reactive, how do we become proactive? How do we get

to a point where we're willing to fail a little because we're going to learn a lot. Bringing those requirements back into the design phase, that's got to be the CONOPS and it's got to be funded. What often happens, even when those cyber requirements are there, all of a sudden they get prioritized out. They've got to be prioritized in. So building that resiliency in, be willing to fail a little so you learn a lot, and you incorporate those resiliency facts into your systems, and then continuing to work as one team. It's not us against them. It's, "Hey, we are one team." And getting to the best answer will help us in changing that CONOPS to get ahead of the ready, as opposed to, we're in our reaction mode.

Quinn Bottum:

So I think on two different levels, that AI and ML can play a role in development. I think first, if you look at a lot of... If you look at some of the exploits and some of the offensive capabilities that are out there, one of the things that you'll see quite a bit of is assembly code. There's a lot of assembly code and machine language that is used to write these tools. But then, if we go back to the talent question we're bringing up, the vast majority of college and even graduate curriculums, they're not teaching assembly right now. You see kids come out and they write C, maybe. They write a lot of Python. They don't write assembly. And so that right there, I doubt that's going to change anytime soon because Python and C, that's what's sexy to write. And C is even not that fun for a lot of kids to write anymore.

But that's an area where AI and ML might have a role. Assembly can be discreet. AI and ML have pretty good application to discrete problem sets. Finding ways of using it to actually compile code into whatever's been written into assembly could help from a capability perspective. And then, in terms of how you use that in a CONOP development, I'll go back to something I said a little bit earlier. We have to find ways of coordinating and orchestrating these defensive capabilities. And if we're going to be proactive, if we're going to try to maneuver the cyberspace towards positions from which we have the advantage, that maybe we can drive, we can postpone needing to be resilient for as long as possible. Not to say we're not going to have to be resilient, but postpone it for at least a few minutes.

Reinforcement learning is a phenomenal application, has a great application towards probabilistically taking steps. It's where it first really came into, at least in the public sphere, it's fame was in when it was playing, Go. When it beat a human in Go. And that's nothing but a back and forth. That's a great way that can be abstracted into how do you take defensive systems that have been built by Leidos, by whoever, and all of a sudden make them actually work together because the machine is actually the one that is exchanging the information between the systems and adapting how the systems are actually prepared to defend faster than the attacker can actually take the information that they've gained and actually use it to craft their next attack. So I think those are the two that I'd highlight. But Tom, you've got a lot of experience in this, so I'd be curious to hear what you think there.

Thomas P. Michelli:

I'm just rubbing off of Tish, you and Quinn. So Quinn, you talked about the assembly. So one of the things too is for speed and agility and perpetual movement and improvement, the software build materials. So going back to the whole of nation all the way from a prime down to a sub, a individual who's new into the business that we want to get their intelligences. Having a standard way of getting some sense of level of security in all the pieces parts that we put into the system. And then, the other thing is, when I first got into this business, I was a real estate IT guy and I got into government because I was a army guardsman who really enjoyed doing offensive, defensive stuff in OAF102. But then I would get into exercises and the first thing that we would wave a magic hand over was cyber.

We couldn't bring down networks because that would impact the pilots being able to fly their missions. Well, that's the whole point. But they would've gotten to fly their mission. So we just waved a hand over

the cyber stuff. So the other thing is, you'd mentioned about exercising and learning how to do AI, ML in an actual exercise where cyber really matters. If we've teed up 10,000 partners, 10,000 people in an exercise with our allies and partners and we shut it down because we didn't do cyber right, we should learn lesson from that. So the other part is exercising for real resiliency and how we're going to fight hurt with our allies and partners.

Maj. Gen. Anthony Genatempo:

Outstanding. All right. We have a few minutes left. The doors are still locked from the outside and you have a captive audience. Closing comments on resiliency, workforce, imagination, to share with the audience.

Latisha R. Rourke:

Sure. Thanks for inviting me to be part of this panel. Great discussion that we've had. Great to meet two great peers in the industry. We all know it, we experience it every day, engaging and continuing to make cyber a priority in our platforms and in our systems and in defending our nation and the homeland, is got to be a priority. Without it, the rest of the domains, air, sea, land, and space, as Tom just said, they don't have that connectivity and we've got to get ahead of that. So make cyber a priority.

Thomas P. Michelli:

Yeah, again, engage everybody. Find ways to work with our contracting officers to do demos, to bring demonstrations in, to work with our allies and partners and get their great companies into what we're doing and get what we're doing to our allies and partners. Exercise. Make exercise real. Really work through the resiliency and transport, confidentiality, integrity of our systems. And back to boiling the frog, every time you take a risk, a small risk, because you think somebody else has taken care of it for you, for you and you're left or right or up and down, look at the big picture because pretty soon, that temperature gets so high and the risk gets so great, you've boiled the frog. In other words, you no longer have a mission capable system that you can fight hurt.

Quinn Bottum:

So [inaudible 00:35:58], thank you very much for the opportunity and it's been great to meet both of you and thanks General, for the opportunity for leading us here. I think, the last thing I'll say is I'll build upon that. As we exercise and as we look at risk, as we see that the temperature rising. I think for everyone in this community, it's a matter of, can we raise the discourse around cybersecurity? Can we try to start to remove some of the generalizations, the statements without context and actually start driving it more nuanced discussions. Because as we do that, I think that speaks to the harder resiliency where we start to acknowledge the fact that our systems are not likely going to be as secure as we want them to be.

No matter how hard we try or how much money we throw into it, there will be holes and we will have adverse situations occur. So if we're open and we talk in more nuanced level about where the actual issues are and why they're arising and how we mitigate them today and in the future, we recognize the issues that legacy presents and we figure out, we actually start to look at resiliency from an eyes wide open approach. I think that's something that this, as a community, will find results a lot faster than we think we will.

Maj. Gen. Anthony Genatempo:

All right, thank you Quinn, Tish, Tom. I appreciate your patience with a brand new member of the cyber enterprise standing here at the podium. I really appreciate your time here and the conversations that we had. Folks, we are going to step outside. You can find us out there. The chief is actually going to be in this room right after us. So we're just going to move out to the front and the side. I'd like to give our panelists of big round of applause for their time.