Transcript

National Guard Bureau Public Affairs
Press Desk (703) 601-6767
ng.ncr.ngb-arng.mesg.ngb-media-desk-owner@army.mil
www.nationalguard.mil

NATIONAL GUARD ON-THE-RECORD TELEPHONIC MEDIA ROUNDTABLE

JUNE 7, 2022

TOPIC	SUBJECT MATTER EXPERTS
National Guard Cyber Shield 2022	▪ Air Force Maj. Gen. Richard Neely, Adjutant General of Illinois and Commander of the Illinois National Guard and a Master Cyber Space Officer. ▪ Mr. George Battistelli, exercise director and Deputy Chief Information Officer, ARNG ▪ Army Lt. Col. Jeffrey Fleming (ILARNG), exercise Officer in Charge. ▪ Army Lt. Col. Carla Raisler (KYARNG), exercise Training Officer ▪ Army Capt. Cumah Blake (MNARNG), exercise Staff Judge Advocate

Introduction:

Our nation, states, communities, corporations and institutions are under attack each and every day; but rather than bombs and bullets our adversaries are using binary ones and zeros. And, just as it has for more than 380 years, the National Guard is playing a key role our defense.

The National Guard is conducting its annual unclassified Cyber Shield exercise June 5-17 at the Army National Guard Professional Education Center on Camp Joseph T. Robinson Maneuver Training Center, North Little Rock, Arkansas. This annual exercise began in 2007 and involves more than 800 National Guard Soldiers and Airmen from throughout the United States and its territories as well as partners from other government agencies and the private sector.

The exercise is a result of the National Guard's commitment to defend critical infrastructure from the growing threat of cyber assaults. It is conducted in an unclassified environment to allow for more involvement from partners outside the Department of Defense. The mission of Cyber Shield is to develop, train and exercise cyber forces in the areas of computer network internal defensive measures and cyber incident response. These capabilities facilitate National Guard Cyber Teams' abilities to conduct missions to coordinate, train and assist federal, state and industry network owners that are threatened by cyberattack.

The focus of this year's exercise is on the National Guard's role in protecting U.S. Department of Defense computer networks. In addition to assisting outside agencies, the civilian-acquired skills that many cyber National Guard members possess also strengthens the military's ability to protect the

military's own networks against attack. As in defense of external networks, relationships and communication established outside the military, but within the bounds of operational security, are important in defense of the military's computer networks.

The on-the-record telephonic media roundtable was conducted Tuesday, June 7, from 11-11:45 a.m. (EDT).

Dialogue:

[Name]	**[QUESTION/RESPONSE]**
Mr. Wayne Hall	Good morning, ladies and gentlemen, members of the media, thank you for joining us for today's Media Roundtable, focusing on the National Guard's cybersecurity mission through Exercise Shield 2022. Before we begin, I want to remind everyone that this event is on the record. Our nation states, communities, corporations and institutions are under attack each and every day. But rather than be. But rather than bombs and bullets, our adversaries are using binary ones and zeros. And just as it has more than 300 New Years, the National Guard is playing a key role in our defense. The National Guard is conducting its annual unclassified cyber shield exercise June 5th through 17th at the Army National Guard Professional Education Center on Camp Joseph Robinson, Maneuver Center, Training Center, North Little Rock, Arkansas. Today we have with us Major General richard Neely, adjutant general, Illinois National Guard and a master cyberspace officer. Mr. George Battistelli, exercise director and deputy Chief Information Officer, Army National Guard. Lieutenant Colonel Jeffrey Fleming. Illinois Army National Guard. Who is the exercise officer in charge. We have Lieutenant Colonel Carla Raisler, Kentucky National Guard, who is the exercise training officer, and Captain Cumah Blake from the Minnesota National Guard, who is exercise staff judge advocate. This roundtable will last approximately 45 minutes. We'll begin with opening remarks and introductions from the panel members. Major General Neely, over to you, sir.
Maj. Gen. Richard Neely	Well. Good morning, everyone. Thank you for that introduction. So when we talk about cyber attacks, whether it's state sponsored, independent criminals. We've all seen these attacks attack not only some of our private infrastructure, but our critical infrastructure at every state and department as well as within the Department of Defense. If I look back to my own state of Illinois, just in the past month, the City of Quincy Municipality Network was hobbled by ransomware attacks. Last year, the Illinois Attorney General's computer networks were also

attacked. And as many of you are probably aware, the Illinois Board of Elections Network was attacked in 2016, as well as several other states. As a result, the Illinois National Guard has been working working closely with the Board of Elections in cyber defense. The National Guard is uniquely situated to assist with these types of attacks from outside the military network. Our state and federal mission, as well as our citizens, soldiers and airmen, bring in civilian-acquired skills that are tremendous to help in this regard. What isn't discussed as much is how those uniquenesses of the National Guard also help the federal mission of protecting the Department of Defense and the federal government networks. Those same civilian-acquired skills such as working in a private industry, those relationships with educational institutions, relationships with tech sectors such as some of the largest tech sectors in our country and the corporate industrial world is invaluable for our primary mission of protecting our own networks. Cyber Shield 2022 is putting the spotlight on that primary mission this year. The Department of Defense and the private sector need to continue to work together to develop cyber defense together, to share best practices in protecting our infrastructure. Knowing that 85% of all our critical infrastructure is owned in the private sector, the SolarWinds attack that was discovered in December of 2020 is what we refer to as the supply chain attack. Just demonstrating the importance of this type of collaboration. That sophisticated. And most likely state-sponsored, attack hit both private and government networks. Protecting against these attacks like this will also require collaboration. As with all other emergencies, it's not a good idea to be trading business cards in the middle of a crisis. It's all about planning and training together. And that's what's great about Cyber Shield. Cyber Shield is special because it integrates at all levels of government, tech, industry, law enforcement and other partners. These military cyber warriors have a significant advantage over their active-duty counterparts as they bring in those unique civilian acquired skills and experiences in addition to their military cyber training. This year's exercise will have 20 participants, 20 states participating, as well as Guam. And the private sector will also be involved, as well as some of our top-notch educational institutions from across our country. From the Department of Defense, we will have the Navy also involved, as well as Coast Guard from Homeland Security. We also have a special workshop with several of our National Guard state partnership countries as they get a glimpse into how we manage cyber defense operations. These organizations came to the table because some of our cyber warriors from individual states asked them to participate. This really gets to the

strength of the National Guard as a community-based organization and how we can connect to be the connective tissue between the Department of Defense in our communities, across our nation, to ensure that our nation is protected. In some cases, some of the National Guard cyber warriors work in the same organizations that are now participating in Cyber Shield. It is said no problem is solved from top down. The best solutions come from those who are solving it and then it's implemented across the organization. This is true with Cyber Shield. This exercise started several years ago with just a few cyber soldiers getting together to try to fill some training gaps. And it has evolved into it evolved into one of the largest unclassified cyber training exercises in the military with more than 800 participants. It is, it continues to evolve and we will continue to evolve the exercise as it threat evolves. So with that, I will pause for Mr. Battistelli to make a few comments about this year's cyber exercise. Thank you.

George Battistelli

Hey. Good morning, everybody. I'm George Battistelli. I am the deputy chief information officer for the Army National Guard, and I'm also the Cyber Shield Exercise director. So thanks to Major General Neely for excellent scene setting and opening comments. Really appreciate that, sir. Appreciate your leadership. For the last several years, we've experienced multiple challenges in the United States that our cyber adversaries have taken the opportunity to seize upon. We saw it during the 2016 and 2020 presidential elections, where foreign attempts to spread disinformation were rampant in an attempt to disrupt the democratic process and distract and divide the American people. It also became a factor during the COVID-19 pandemic, where disinformation was again being spread. Social media has changed the way we communicate and consume data in that manner. It's important for us to continue to train our soldiers using real-world events so they're able to cut down the noise and focus on their mission for the exercise. And in the real world, we strive to achieve and maintain information advantage over our adversaries. For Cyber Shield 2022, we have a simulated social media platform on the cyber range the teams will have to pay attention to so they can potentially glean information or disinformation as they conduct their hunt, clear, defend mission. This year, our scenario is a SolarWinds-like supply chain event, where the teams will simulate a response on the Department of Defense Information Network, also referred to as the DoDIN. In past events, we focused more on election support or critical infrastructure protection. However, once SolarWinds

	kicked off, and to a lesser extent Log4J, it became clear that we needed to focus on responding to an event on the DoD. This is because the authorities are different depending on what status our soldiers are in, whether they're in a state active duty status, Title 32 or Title 10, which is why having a JAG on our leadership staff is critical. In addition, the incident response toolkits are different for a response in the DoD and versus a state active duty response. For example, some open source tools that are readily available and used on a state active duty response are not approved for use in the DoD. As Major General Neely stated in the National Guard, we have some of the most talented cyber warriors in the Department of Defense. This is because many of our soldiers on orders for this event are industry leaders in their respective field when not on orders. I am always amazed by the breadth and depth of knowledge these soldiers bring and their thirst for continued knowledge. I learn something every year and I am always confident to come back. I feel confident that these are the teams defending our cyber landscape. They understand the environment. They protect the boundaries, and they defend it from all adversaries. With that, I'll turn it over to the soldier who's making this operation go, the exercise. OIC [Officer in Charge], who I give the commander's intent to and he moves out swimmingly. Lieutenant Colonel Jeff Fleming.
Lt. Col. Jeffrey Fleming	Hey. Good morning. I'm Lieutenant Colonel Jeff Fleming from the Illinois Army National Guard. And I'm serving as this year's officer in charge of Cyber Shield.
Lt. Col. Carla Raisler	Good morning. I'm Lieutenant Colonel Carla Raisler with the Kentucky National Guard. This is my 6th year participating in Cyber Shield. I've had several positions, including team leader assessment. And this year, I'm the training officer responsible for educating and training our information assurance workforce.
Capt. Cumah Blake	Good morning. I'm Captain Cumah Blake with the Minnesota National Guard and serving as the staff judge advocate for the exercise. My role is to help implementing the legal considerations into the planning of the exercise. And during the exercise I provide technical oversight of the judge advocate participating and advising the teams.
Wayne Hall	Thank you all. So with that, we would respectfully ask that all participants please state their name and affiliation before asking a question; and being respectful of time, we ask that media please keep to

	one question with a follow up. We will allow for additional questions should time permit. If we are unable to address your question, we will take note of it and get to get you an answer as soon as we can following the roundtable. All right. So first, we'll go to CNN. Ellie Kauffman, are you with us? Do you have a question? Ellie. All right. Not hearing anything. We'll move on to CBS. Eleanor Watson, are you with us? And you have a question?
Eleanor Watson	Wayne I'm here. I just have a quick question on the workshop with the State Partnership Program, which, um, which countries are participating in that workshop? And can you give me a little more details about the workshop? Thank you.
Wayne Hall	So. Yes, so I'm going to go to Lieutenant Colonel Fleming. Sir, would you mind addressing that question?
Lt. Col. Jeffrey Fleming	Yes. Thank you. So the SPP, as you can imagine, with the global events going on the RSVPs are still flowing in. So, we don't have a final confirmed list of attendees yet. But what that workshop generally consists of we bring in speakers from across the DoD or some of our civilian partners and just kind of discuss with them and show them this is how we conduct a cyber exercise. These are the things we include. We talk to them about a little bit how we get to the planning of it; different features that we have at it; and then talk about the execution of the event itself. And then the follow-on or end of that is we'll actually walk them around and show them some of the stuff that we can so they can get eyes-on and generate additional questions so that they can go home and work to replicate this with their state partner back in their own forces.
Wayne Hall	Thank you.
Maj. Gen. Richard Neely	If I could just add to that, I think what's important about this workshop is so many times the United States looked at as some of the best for cyber security and cyber defense and what it does with our state partners, it really provides a new level of confidence when they come in and see not only the workshop but again, the unclassified collaboration that occurs at Cyber Shield. I think that's the most important ingredient there. When they go back and try to implement this collaboration, this planning and training that Jeff mentioned just a few minutes ago. Thank you.

Transcript

National Guard Bureau Public Affairs
Press Desk (703) 601-6767
ng.ncr.ngb-arng.mesg.ngb-media-desk-owner@army.mil
www.nationalguard.mil

Wayne Hall	Thank you. All right. So we'll go over to next question, ABC News Matt Seyler, are you there and do you have a question?
Matthew Seyler	I ... No question for me.
Wayne Hall	Thank you. All right, Matt, thank you.
George Battistelli	Hey, Wayne, you're on mute.
Wayne Hall	Thank you. It wouldn't be a zoom without a mute malfunction. Steve Beynon from Military.com, are you online? Do you have a question? Steve. All right. Nothing herd. I'm going to go ahead and move on. IOCI Radio. Are you online? If you have a question. IOCI Radio. Kim Howard, are you online? Hey, moving on. WSIU Benjy Jeffords. Are you on line? If you have a question. Benjy.
Benjy Jeffords	I'm here.
Wayne Hall	Do you have a question, sir?
Benjy Jeffords	Not right now, I don't.
Wayne Hall	All right. Thank you. All right. We will go to C4ISRNET colin Demarest, are you online and do you have a question? Colin, are you there? Nothing heard. Kari Williams, Reserve and National Guard magazine. Are you online and do you have a question?
Kari Williams	Yes, I am. Thank you. I was just wondering how the command cyber readiness inspection program that relates to the training and things going on over the next few days with Cyber Shield or if it does at all.
George Battistelli	Hey, Wayne, I can take that one. So thanks for that question, Kari. One of the things that we've looked at for Cyber Shield specifically is how do we continue to to harden our enterprise? And we look at the command's cyber readiness inspection. I look at that almost as a compliance-based inspection, whereas for for Cyber Shield, we're really trying to train the defensive cyber operations personnel. So while they're looking at whether the devices are hardened as they're going through all of their scanning and they're trying to determine where the boundary is and where they're protecting, I think the command cyber readiness inspection is just a little bit different because the command cyber readiness

	inspection is really some of your cyber hygiene. And while we do have a cyber hygiene team in the the Army National Guard, this event is really more focused on training our defensive cyber operations warrior so that they when they respond to an event, they they understand what the requirements are over.
Wayne Hall	Thank you, anybody else like to add to that?
Lt. Col. Carla Raisler	This is Colonel Raisler. So when we talk about with the training, we have 15 different courses, as Mr. Battistelli mentioned. We're working towards our being able to improve the ability for our cyber warriors to respond to incident responses, either on the DoDIN or in a civilian capacity. Those classes are industry-level courses such as security-plus, incident responder handler's courses, teaching them the basics on when they get on the network. What type of things are they looking for and how can they respond?
Wayne Hall	Thank you, ma'am. Next, we'll move on to WAND TV. Caryn Eisert, are you online and do you have a question? Caryn. All right. Nothing heard. Alexandria, Alexandria. Kelly from NextGov, you online? Do you have a question?
Alexandria Kelly	Hi. I'm on mute. Nothing for me right now. Thank you.
Wayne Hall	All right. Thank you. KMOX Radio Audacy. Megan Lynch, are you online? Do you have a question?
Megan Lynch	I am. Yes. Thank you very much. I do have a question. You know, when we're talking about the SolarWinds incursion, we're talking about an incident of a commonly-used software. So I'm curious for Cyber Shield, when you're running through these exercises, what are you looking at from the time frame? Maybe of the point a glitch is discovered and someone tries to take advantage of that to the time. You have to keep them from executing that on a system.
Wayne Hall	Mr. Battistelli.
George Battistelli	I'll take the first part of that and then I'll kick it over to Jeff Fleming and team for the second part of that. And so thanks Megan. A lot of times what we tell people, especially for any kind of cyber incident response, is that the first thing you want to do is take a deep breath. A lot of times the

event has already happened. We are really detecting it after the event has happened. And so we are at that point trying to determine what the scope and the scale is. And so now the difference for us specifically in defensive cyber operations is that we're always on defense and we have to be right 100% of the time, and the adversary only has to be right one time to get through. And so as far as the technical pieces and parts of how we're doing that, I'd kick that over to Lieutenant Colonel Fleming and team and let them talk further on that over.

Lt. Col. Jeffrey Fleming — Yeah. Hey, thanks, George. Um, so as far as the specifics. So the scenario evolves every year depending on guidance from Cyber Command, National Guard Bureau and the events taking place in the world. So this year specifically is, as we said earlier, it is a supply chain type attack. And the the blue teams this year will be walking into a network and they know they're showing up for incident response. So we've done some different things in years past, but this year they're showing up, hey, you know, you know, something's happened and they need to show up and respond to it. One of the great things that has evolved over the years from some of the experts that are here is the team doing the adversary emulation ... in playing the bad guys is very keen to make sure the blue teams all come away with something. We understand across the different 54, there's varying skill levels and experience levels. And so the group that we call the red team, they are, they go into the blue team cells and help them out. So to your point about how are they finding these things and different things like that? So for our newer teams that struggle, we have what we call a purple day. And so the red team will go in there and show them, hey, this is this is where the attack started. This is where you should have caught it. These are some of the different ways you can have seen it, and then they'll talk through them if time is available to do some of the remediation for those events.

Megan Lynch — Fantastic.

Wayne Hall — Anybody else have anything to add to that?

Megan Lynch — Sorry.

Wayne Hall — No go ahead. Do you have a follow up?

Megan Lynch — Yeah, I was going to ask a follow up. You know, you mentioned the world events. Obviously, we can't ignore what's going on in Russia, in

Ukraine right now with Russia. So, you know, what are your teams looking at that and, you know, watching what's happening there as instructive in in what you're doing for this exercise?

George Battistelli

Absolutely so. So I can answer that. And then I'd like to to push it over to two Major General Neely to get some comments on that as well. But every year when we plan the exercise where we're planning the exercise, we planned it about a year out. And so we're looking at events that are happening at that point. And really by the time we get to the exercise, it's almost obsolete because so much happens in a year in cyber as we're we're trying to to plan for these things. But we're all watching what's what's happening in Ukraine and, you know, obviously keeping abreast of that. But this exercise is specifically focused on defensive cyber operations capability. And so we're really looking at defense of the DoDIN, and that could be defense from anywhere, whether it's, you know, foreign, domestic, somebody who stumbles on to the wrong thing and starts to send a storm towards the network and, you know, something that's misconfigured. And so we're certainly keeping an eye on it, but it's not something that we've specifically built our scenario around this year. But I'd like to send it over to Major General Neely for a state perspective. Over.

Maj. Gen. Richard Neely

Thank you. Mr. Battistelli those are excellent comments. And I would just add to that is I really you know, what we're watching from afar occurring in Ukraine is something that's bringing us all together. And it really highlights Cyber Shield for us because what we've seen on, you know, our nation do is is really begin to collaborate at a much higher level. Rather, it's the release of information. And we talk a little bit about misinformation and disinformation early on as Mr. Battistelli in his open comments. But it helps us to become to have this awareness that we need to collaborate more closely state, local, private sector, federal government, Department of Defense, all of us have to be talking about these attacks and where these are coming from. And we know that are rather we're talking about a zero-day issue or we're talking about state-sponsored attacks on our critical infrastructure structure. The more that we're aware and the more that we're communicating and the more we're knocking down disinformation and misinformation, we're all better off. And this really brings us together. I know my Department of Innovation and Technology from the state of Illinois, you know, we work very closely with them on a regular basis, rather, as I mentioned earlier, with the election security. But we also work with them whenever there is one

	of these ransomware attacks, they may respond to it. But we maintain our awareness. We try to bring in best practices and help. And that relationship all began at a Cyber Shield; and I cannot emphasize, you know, the greatness of coming together at one of these exercises and bringing those other entities together to work together at one of these events. And so I think we can all take a page from what's happening today and continuing to develop our collaboration. Thank you.
Wayne Hall	Thank you, sir. Next, we'll go over to I'm sorry.
Lt. Col. Jeffrey Fleming	Supposed to say I just had one more.
Wayne Hall	Oh, please. By all means.
Lt. Col. Jeffrey Fleming	Yes. So one of the things you know is it again, was mentioned earlier about that, you know, this is the most professional group that that brings extra civilian skills to that. So to address those unknown threats that haven't popped up yet or haven't been discovered, as well as the evolving threats from wherever they come from. Our red team has some of the best folks in the industry, and they're able to recruit additional better folks to come challenge our blue teams. So I can't go too far into this year because I want the blue teams to get too much information ahead of time. But last year, one of our red teamers actually wrote their own piece of software to throw against the blue teams. So something that they would have had to find from scratch that wasn't out there. And additionally, last year, they brought a bug bounty hunter who had proof of concept code for a zero-day that he was able to test our blue teams against. So we do provide them a world-class set of threat emulators to challenge them at the highest levels to prepare for those those advanced threats.
Wayne Hall	All right. Thank you, sir. Next, we'll go to Dave Dahl with WTAX Radio. Are you on the line, sir? Do you have a question?
NGB-PA (for Dave Dahl)	Hey, this. Dave Yocum, I'm going to speak for Mr. Dahl here. I have a question. Good morning. It's Dave Dahl from WTAX Radio in Springfield, Illinois. General Neely, can you please recap what's happened good and bad, in cybersecurity since last year's event? Thank you so much.

Transcript

National Guard Bureau Public Affairs
Press Desk (703) 601-6767
ng.ncr.ngb-arng.mesg.ngb-media-desk-owner@army.mil
www.nationalguard.mil

Maj. Gen. Richard Neely

Well, that's a broad statement, but thanks for that, David. Thanks for joining us, as always. You know, I think the Ukraine, Ukraine war that's going on with Russia attacking Ukraine, I think is, as I just highlighted a few minutes ago, the collaboration that I've seen from the ways CISA Cybersecurity and Infrastructure Security Security Agency has as pulled together is is really a highlight that I've watched over this this last year. And you know, my working with the both here in the state of Illinois and at the federal level, I've seen the collaboration become much closer and much tighter with whether it's information sharing or if it's preparedness awareness of the new zero-days and that there's some things that have come out policy wise over the last several years that are now we're starting to see take effect. That I think is really helping us all to better understand from a policy, a legal perspective as well as more of a focus on our critical infrastructure, help us all to have a better awareness and, and increase our security overall of our nation. That, again, I made reference to 85% of our critical infrastructure is owned by private sector. So we we have to when we talk about, you know, power or water systems that we depend on, transportation that we depend on. So much of this is not owned by the government. And so we have to depend on others to ensure that their their cybersecurity is up to snuff, too, for life and safety of those. Hopefully that helps.

Wayne Hall

Thank you, sir. All right. So next, we'll go to ABC-7 out of Chicago. Jeff, Markchese. If I've got that name incorrect I apologize. Are you online or do you have a question? Jeff. Hey, nothing herd so I'm going to go ahead and move on to Matthew Whitlock from WICS. Are you online? Do you have a question, sir? Matthew. Nothing heard. I'm going to go on to WMAY Radio. Jim Leach, are you online and do you have a question, sir? Jim. Nothing heard. We'll move on to GLBT Public Radio, Charlie, are you online or do you have a question? Well moving right along here. All right. With that, I'm going to circle back are there. I'm sorry, KATV Channel 7. I don't think you have your audio on, but are you online and do you have a question? All right. Nothing heard. I'll start to circle back. Are there anybody is there anybody on line who didn't have a question earlier? Who would would like to ask a question? Nothing heard. All right. One last chance. Is there anybody else online who would like to ask a question?

Kari Williams

It’s Kari Williams with AmeriForce Media. I just had one more question, if that's okay.

Wayne Hall	Yes, Kari, go ahead, please.
Kari Williams	Yeah. So I know just within the last couple of weeks or so, the Iowa National Guard held a cyber defense competition as part of its state partnership program with Kosovo. So how do you see like national scale events like Cyber Shield, kind of trickle down to training at the state level? Is that what they did with Iowa and Kosovo kind of an example of that? Or are there other ways that you see that see kind of takeaways from Cyber Shield go down to the state level?
Wayne Hall	I think we have lots of folks who can address that question. I'd like to start with General Neely.
Maj. Gen. Richard Neely	Hey, thank you for that question, Kari. I appreciate that. You know, our state partnership program and I've been involved with it for many years, nearly 30-year partnership with Poland, and we've watched it really evolve throughout those 30 years. And and early on it was about, you know, formation, marching in OCS classes, officer candidate courses and NCO courses and then really developing some of these military to really be part of NATO and other other professional organizations really bringing up their level of maturity as a military organization. And but here, more recently, there's a significant interest in cyber. And again, it goes back to the United States, does a great job of how we try to collaborate, how do we try to get after cyber defense. Mr. Battistelli discussed it earlier about, you know, you have to be 100% right or any hole in the net is going to be be taken advantage of. And so we're constantly looking at how to work that and that our partners from our state partnership programs come to to really see, you know, what we can share. Again, it's this unclassified exercises is an excellent example of how we collaborate and how we work together. And so many it so much of work that we can share with our partners really highlighting the unique, maybe some of the unique steps that we might take. As Colonel Fleming mentioned earlier, that you know, how the red team might attack the blue team that's trying to defend and understanding those techniques that we might use and as well as, even, again, those private-sector unique, unique acquired skills that we bring to that fight. Those are things that I think many of our partners are looking for. How to how do we do that? And so there's a there's a lot of good examples of where we'll continue to work with, I'm working very closely with, I just got done spending several days with my Polish counterpart that in charge of cyber and they're you know they're they're doing their best to make sure

that that they're coming up to speed with the rest of the world because they know cyber defense is really the one of the most significant threats that they have right now. So hopefully that helps out a little bit.

Wayne Hall — Thank you, sir. Mr. Battistelli, do you have anything to add before I go back to the team?

George Battistelli — Yes, certainly so. Unfortunately, I just lost video. Thanks for for Zoom, but as long as you can still hear me, I'm good to go. So you have me on audio?

Wayne Hall — Yes, we got you. Good.

George Battistelli — Okay. Excellent. So one of the things I would say to that is that I appreciate the comments there from Major General Neely. We we envision at the National Guard Bureau that the Cyber Shield exercise is the national-level cyber exercise for the National Guard. One of the things that continues to happen is that we also have regional exercises. So Cyber Yankee is an exercise held in the Northeast corridor where a lot of the northeastern states get together and they work out through their cyber pieces in parts there. And then we have a lot of state-specific exercises. One of the big challenges that we have is that the National Guard we always get it done. We always make things happen. Whether we're under-resourced, undermanned, we continue to complete the mission. And that's become one of our challenges as we've seen the uptick with all of the cyber exercise and the demand signal from cyber, it's always funding. And so we build in and we fund the Cyber Shield exercise. But one of the things that we're continuing to figure out is what the future of these cyber exercises looks like from a funding perspective. Because a lot of times when you're using the range, you're bringing in personnel, these things are expensive. And so we always have our fiduciary responsibilities that we're taking care of as well. But I'd be remiss if I didn't pass it over to the panel to get their input also over.

Wayne Hall — Roger. Thank you, sir. I'm going to go to the panel over at the at the PEC. And I want to start with Captain Blake to ask that question. And it's from the Judge Advocate, Staff judge Advocate approach the to the piece.

Capt. Cumah Blake — Yeah. I think the Cyber Shield exercise is a great model for to bring down to the states and especially with their partnerships. And the reason

I say that is here at the Cyber Shield exercise is not just the cyberspace operators. There is an integrated team. And one of those aspects, for example, is the judge advocates, the attorneys, that are advising the teams on different legal considerations. And so when you do this at a smaller scale with your partnership, you're showing them the model of not only doing cyberspace operation in a vacuum, but how do you integrate with other members of your team that support and make those missions successful? So I think this is a good model that the states can use, especially with their partnerships.

Wayne Hall — Thank you, ma'am. Next.

Lt. Col. Jeffrey Fleming — Yeah. So. So one of the biggest challenges we have is across our 54 states and territories that all have their own ways of doing things and left and right limits that they've been given. Additionally, they share a similar amount or larger amount of state partners all over the world who again have different limitations, capability sets, etc.. So as Captain Blake said, it's a good national set. It's amazing to be back in person this year because one of the things we've lost having the virtual of the last couple of years is that ability for everybody to come here to this national level, exercise and share ideas. And that is one of the you know, the unspoken and really almost the benefits of bringing everybody together is if we have a state that is excelling in one area or has figured out how to work with their attorneys to get through some of the red tape, to get something done, whether it's getting private sector top-level clearances and integrated into state cyber task forces or organizations, or collaborating with state partners in getting them, you know, on state networks and doing combined cyber missions. So if one state's able to do that and figure it out, they can come here to talk about it and share it. And then the rest of the states that have an appetite to do that can take those lessons learned, take those templates and bring them back to their own states and into their state partners to go to do some of that furtherance of ideas and share those ideas across the force.

Wayne Hall — Thank you, sir. Colonel Raisler, anything else to add?

Lt. Col. Carla Raisler — Yes, I think one of the aspects when it comes to partnership and learning is the actually the staff here. So the staff works together for the entire year to build the exercise out. And the vast majority of the staff at this event come year after year. And so we have built our relationships with the different states that we have staff members from. But it also allows

	us to take the information that we learned from building the exercise back to our state and work with our partners there, either state partners or our SPPs, to recreate the events and the training model for them.
Wayne Hall	Thank you, ma'am. Before we go to closing remarks, we have time for one more question, if there's anybody else who would like to ask a question. Anybody else with an additional question. Okay. I've not heard anything. So with that, like to just let folks know we dropped a link to a story on National Guard.mil in the chat window here (https://ngpa.us/20087). That story is up. It's the first story out of cyber shield 2022 that you can pull up and resource as well. As you move forward. And with that, I'm going to go ahead and I'll start with General Neely down through Mr. Battistelli and then the leadership panel for any closing remarks. General Neely, over to you, sir.
Maj. Gen. Richard Neely	Okay. Hey, thanks, Wayne. Knowing to all those who joined us today, thanks for taking time out of your busy schedules to join us for this important media roundtable on Cyber Shield 2022. As you can hear an enthusiasm of our panelists and those joining you today, we really are big believers in the concept of how we collaborate and share this information with cyber defense. And as our nation becomes and our world becomes more of a dangerous place in cyberspace, it's more important than ever to continue this this level of collaboration. Secondly, I'd like to thank the staff for putting this together. And, you know, most everybody with dealing with Cyber Shield is a volunteer. That's an additional duty. Everybody from Mr. Battistelli down to Colonel Fleming and the rest of the team, there are all volunteers who have continued year after year to make sure that cyber shield continues to move forward as a priority because they are believers in it. As Colonel Fleming stated earlier, having it back in person this year is a significant advantage to be able to share those best practices across the National Guard and continue for everybody to bring our game up again, 20 states and the territory of Guam this year participating. So with that, thank you for your time and I'll pause here and turn over to Mr. Battistelli.
George Battistelli	Thank you, sir. Always appreciate your support for the exercise and your leadership and your perspective. So just to kind of close out this year, I made some notes on some things I wanted to make sure that that we covered. And so we already have about 500 packs on site. And in Little Rock at Camp Robinson for the exercise. So as you can see, the panel. They are all on site ar Little Rock. And so very different from years past

where we've gone virtual and we've gone hybrid. Everybody is excited to get back together. We're actually doing an in-person distinguished visitor day on 14 June this year. We haven't been able to do that in the past. And so this is really where the adjutants generals, the different leadership, get to see what their soldiers have accomplished and to see the goodness of the exercise and to see just how technical their soldiers are and what they're learning. And we like to bring the DVs [Designated Visitors] down, and we've got a great threat brief this year. And so we feel like this continues to push the envelope forward, because when we look at the leaders of the different states and Major General Neely is a perfect example. We like to to make sure that they understand exactly what their their cyber soldiers are doing, because there are there are some adjutant generals who have grown up that don't really understand the ones and zeros of cyber and what their soldiers are bringing to the fight. And so we want to make sure that we continue to educate. And so cyber is an education, just like data is an education. So years ago when we said we wanted cyber. Nobody knew what flavor of cyber we wanted, whether it was offensive, defensive, cyber protection team, cyber hygiene assessment team. We're starting to get into that with data now where everybody wants data, but we don't know what we want to do with it. And so we want to build on events like Cyber Shield, and we continue to offer that training not just to the soldiers but also to our senior leaders so that everybody understands. Because if you put me in charge of an aviation crew, I would have no idea what I was doing because that's not my background and not my skill set. And so we call on a lot of the adjutant generals and a lot of the leaders in the Army National Guard and the Air National Guard to be subject matter experts in a wide plethora of areas. And so it's our job to to make sure that we continue to push that information up and help understand and break down some of these technical problems to a non-technical senior leadership staff. And I am part of that non-technical senior leadership staff, but all of the technical folks that are sitting there on the Cyber Shield panel, and so I would push it over to them for closing comments because I really feel like they're the engine that makes it all go over.

Wayne Hall — Thank you, sir. And with that, we'll go back to the leadership team. I would like to start off with Captain Blake.

Capt. Cumah Blake — Yeah. I would just like to close. Like this exercise isn't just about training up our cyberspace operators an opportunity also, for example, to train up our attorneys, our judge advocates, where they're learning the

	language of cyberspace during this exercise and what our operators do. So they're bringing their expertise, but learning the expertise from our cyberspace operators and combining those to make the teams more effective and efficient. So they're coming here, they're learning new skills, new areas of where to apply the law, taking that back home and giving it back to their states and also the operations that they do. So this exercise is not just beneficial to the individual cyber space operations, but the different sections that are supporting those operations and collaborating and being part of the team.
Wayne Hall	Thank you. Lieutenant Colonel Raisler.
Lt. Col. Carla Raisler	Thank you. And while this exercise is based on being able to defend the confidentiality, integrity and availability of our networks, it's also readiness. And by bringing these service members and providing them the industry level training that we provide them, we increase and improve the readiness of our force.
Wayne Hall	Thank you, Lieutenant Colonel Fleming. Over to you, sir.
Lt. Col. Jeffrey Fleming	Yes. Thank you. And so, as Lieutenant Colonel Raisler was saying is, yes, we do. We provide readiness for our federal mission. We provide readiness for the agents, general and the governors to protect the local networks across all of our different mission sets. It's you know, I'm merely to the OIC, but we have a staff here, too. And by another 50 of even more technical expertise than most people can imagine to put this exercise on. And as General Neely said, many of us are M-Day, we do not have a full time assignment to this exercise. We're here because of the passion of want to see it move forward. So that's why this exercise gets better and better every year. But thank everybody for their time for coming today and definitely encourage you to continue to follow the the press releases as the exercise moves forward, especially as we switch from our training week to our exercise week when the stress level goes up just a little bit for some of the defensive teams. And thank you.
Wayne Hall	Thank you, sir. And with that, I'd like to thank our participants this morning and our guests for joining us. For members of the media, if you have additional questions, please feel free to contact us by email. Thank you very much. That concludes today's event.

[End of Audio]

Duration: 47 minutes

For information regarding this transcript, please send an email to the National Guard Bureau Media Operations desk at ng.ncr.ngb-arng.mesg.ngb-media-desk-owner@army.mil.

-30-