Brig. Gen. Gregory Touhill, USAF (Ret.):

Good morning, everybody. All right, for all those folks still talking, good morning. Happy Monday. I'm Greg Touhill. I'll be moderating the Cyber Warfare Panel today, and joining me are some very distinguished members of the cyber community. We've got to my left, General Tim Haugh, we've got Dr. Wanda Jones-Heath, we have General Kevin Kennedy, and Colonel Shay Warakomski. Did I pronounce that correctly or close enough?

Col. Zachary “Shay” Warakomski:

Yes, sir.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Okay, I know him as Shay. I'm Greg Touhill. I'm a retired Air Force Officer and I'm currently serving as the Director of CERT at Carnegie Mellon University. I'm also a Professor of Cybersecurity at Carnegie Mellon University's Heinz College. And today we are going to be talking about one of the more topical issues in the United States and around the world today.

But first I'd like to start with a pop quiz since I'm an academic amongst other things. So how many, by raise of hands, how many of you consider yourselves cyber operators? Raise your hand. Okay. Every single fricking hand ought to be up in this audience. I double dog dare you to identify a single specialty code in the United States military or any job or position in society today that is not touched by cyber and cyber effects. Now let's take this test again. How many of you consider yourself cyber operators? Show me with a raise of hands. Okay, we still have some folks that are going to have to recycle through with the training.

Now I will apologize for those of you who recognize me looking like this. I do have an age-related disability. I can't see up close anymore so I'm going to take out the cheaters. Our rules of engagement for today's panel... And once again, I'm apologizing to my panelists for having to use the Phil Donahue microphones. My rules of engagement for today is I'm going to ask a question, I'm going to direct it to various members of the panel because each one comes with a unique perspective. We've got representation from Joint, from Service, from Headquarters, and from our new Space Force as well. Each one has a different perspective, but it's all part of an integrated approach to cyber operations across the Department of Defense.

So we're going to start with doctrine. Okay. Anybody volunteer to be the first to answer? Okay, I'll do a volunteer. So General George Washington, when he was finishing up his tour of duty as the President of the United States, famously said in his first annual address actually to the Houses of Congress, "To be prepared for war is one of the most effectual means of preserving peace."

So our question, I'm going to direct this to General Haugh first. General, given the fact that we see malicious cyber operations directed against the United States Government, military, economy, and its citizenry, and some of these operations emanate from groups attributed to nation-state sponsored actors and organized cybercriminal groups, do you believe that we are adequately prepared to deter cyber aggression against our country, and if not, how can we do better?

Lt. Gen. Timothy D. Haugh:

Greg, thanks to you. Thanks to the AFA team for letting us address all of the cyber topics that we're going to go through today. I think, Greg, when I think about malicious cyber actors, General Nakasone, last week he spoke at Billington Cybersecurity Summit and really reflected on what does it look like today in terms of our partnerships. And from Cyber Command, our number one partner is the National

Security Agency and you think of the evolution of the partnership between NSA and Cyber Command, much of that is about sharing data and how we share intelligence and share information with our partners in the inter-agency, our international partners, and certainly the unity of effort that we seek across the Department of Defense.

But when you think about the state of partnerships, when General Nakasone took command, there was not a CISA as an agency for DHS. And so how much has evolved over the last five years in terms of partnerships? We're proud of those partnerships and we think that the partnerships that we have across the inter-agency with our international partners, based on information sharing really set that foundation for how we're able to counter threats as we go forward.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Thank you sir. And I was at the Billington event last week and heard General Nakasone's take. I know, Doctor, you were there as well. What are your thoughts as the principal advisor to the secretary of the Air Force on all things cyber? What's your thought?

Dr. Wanda T. Jones-Heath:

Thank you for that. And Tim talked about our partnerships. So I wanted to double down on that. And one of the things that we did in 2022 is the partnership across the DAF looking at are we cyber ready? Are we modernizing enough? How are we investing in the things that we hold near and dear? That's a long effort and we proved in a four month effort through Taskforce Sentinel Stand and Operational Imperative number seven that we have a lot of work to do. That was the start of really understanding what we look like from a cyber posture perspective. We're not done yet. We did some investments. The secretary really put some money down on the table in 2024 for our palm, so we are on our way.

But what I would say is it takes everyone. Greg started the conversation with asking a question, right? Who are cyber operators? I would say everyone. I certainly agree with that and we all have a part to play no matter what functional you're in, because at the end of the day it's about the mission and we're all part of the mission.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Thank you ma'am. General Kennedy, what's your take as the Air Force's Commander of Cyber Forces?

Lt. Gen. Kevin B. Kennedy:

All right, thanks Greg. I kind of want to take a rift off of both what Dr. Jones-Heath and General Haugh said just now is that if you think through the building the partnerships and also support to the Air Force. And so how do we support General Nakasone and General Haugh and how do we support the Chief and the Secretary? It's really the operational level design in competition today. If you think through the question that General Touhill asked about how do we deter? Well, we align operation level under integrated deterrence, right? That's the overarching concept.

Operationally, our job in 16th Air Force as well as our hats that we wear in support of four COCOMs and the United States Air Force is how do we help make the Air Force's capability more to deny the adversary strategy? That is our contributions. We do that with building partners and allies, but within ours we think, how can we ensure that our cyber enterprise is resilient in the United States Air Force? How can we generate combat power? And that's a lot of the work that was done in OI 7, like Dr. Jones-Heath mentioned.

And the other portion on with support the combat and commands. How do we ensure that their mission's resilient with the alignment of cyber protection teams out on key terrain to assure their mission as well as how do we disrupt and expose the adversary, not with just our cyber forces in 16th Air Force, but all the forces in 16th Air Force include our ISR, our EW and IO forces that we have. So we really look at that operational level and how we can support the United States Air Force as well as Cyber Command, EUCOM, STRATCOM, and Space Command.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Thank you sir. Now Shay, you are the senior cyber officer in US Space Force. Space Force is our newest operational service and it's completely different domain. I've done a lot of space stuff, I've got the schwings as well as the cyber wings. The game changes slightly but maybe not so much when we talk about the space domain. How would you answer the question from the space perspective?

Col. Zachary “Shay” Warakomski:

Yeah, good morning. First and foremost, it's a pleasure. I want to thank AFA and certainly to be up here with this very august group of leaders. I tell you what, from our perspective, what's very important to understand is that our operators are employed in place and so we fight from our installations.

They are power projection platforms and so that is the focus. And so this really hearkens back to readiness and resilience across the board. And when you look at resilience, it's the mastery of the defensive and the offensive and the full spectrum cyber operations across the board. And when we're able to do that to properly defend our cyber terrain, we build in that resilience naturally, of course. And that is essentially deterrence by denial.

And then of course when you layer on these additional capabilities that we have, we're able to impose costs and we're able to effect... basically put our adversaries assets at risk. It's very important and that's all part and parcel to this integrated deterrence concept and we're doing it from a position of strength.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Well thank you so much for that. Now we're going to do a follow-up here and pivot over to talking about cyberspace integrated operations. And many senior military and government leaders, myself included, have used the phrase, "Cyber is a team sport" to describe the fact that cyber activities involve many occupational specialties and as we saw from our pop quiz earlier today, we all need to work on that. But also many organizations as well. Many specialties, many organizations. So given that as we look to building our cyber teams, I had like to ask... We'll start with General Kennedy here. Sir, how do you assess we're doing in our efforts to integrate cyberspace operations for unity of effort and maximum positive effects?

Lt. Gen. Kevin B. Kennedy:

All right, thanks Greg. I think we have the frameworks in place and we are definitely on the path of how we think through of how we would integrate. For me, when you start any kind of military capability and you think across domains, you generally start with some level of just deconfliction. You move it into some level of maybe coordination, synchronization, and then you want full on synergy of the forces to get some effects and upscale it.

Where I'd say we are right now is we're... Across the force and the joint force, I'd say we're definitely in the coordination to synchronization line, I think as we've learned. I think that's where I would put us right now. And the mechanisms that we use is cyber is different but not special. And so we think about the effects that we can create in the cyber domain, aligning those into crisis and conflict type of planning

in the normal processes that exist within the combat and commands for aligning those capabilities. Within the cyber area, sometimes those authorities, it's always a coordination across whether it's a functional or a global like Cyber Command and global command or geographic, let's say EUCOM, there's coordination. The question usually comes down to who signs last, right? Who has timing and tempo. All involved, all is in the planning and needs to integrate with both commands, joint fires of processes. But the question on timing and tempo goes to who has the UCP mission and then who is the person that has to execute that mission and align it with the effects and the other domains.

So I'd say we're moving along, we're not in full synergy yet, but I think we're definitely on that line between coordination and synchronization.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Okay, thank you. Let's go over to our space rep. Shay, what do you think?

Col. Zachary “Shay” Warakomski:

Yeah, so absolutely at the heart of the nexus of the space and cyber domains, I think you'll find they're not only inextricably linked, but they're actually reciprocally enabling. And what do I mean by that? So often we talk about cyber enabled space operations, in particular for terrestrial effects and objectives across the board. You can flip that paradigm just a little bit from the standpoint of offering a wider array of exquisite capabilities for the combat and commanders and our nation's leadership through space enabled cyber operations as well. And when you take into consideration the entire portfolio of information warfare and electronic warfare in timing and tempo as General Kennedy alluded to, that hosts a whole lot of arrows in the quiver for our nation's leadership.

And I'll tell you I'm most... I'm excited about the partnership that we have not only with 16th Air Force, with General Kennedy and his team, to be able to get after some of those full spectrum operations, but in particular we've just stood up in Integrated Mission Analysis team out at US Cyber Command. So thank you to General Haugh as well as the rest of CYBERCOM as we look to stand up the Space Force Service component to each combat and command across the board. But in particular we will have that direct connective tissue with US CYBERCOM.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Thank you. Doctor.

Dr. Wanda T. Jones-Heath:

Just want to add one point. Before we actually execute, right? We already talked about teamwork and collaboration and synchronization. Part of it is being able to exercise those options prior to going to war. We're starting to do a lot of that. You see in PACOM region, a lot of joint exercises. We don't fight by ourself. This include our sister services. So we have to keep that in mind as we think about are we able to project enough power both in the Air and Space Force.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Thank you. General?

Lt. Gen. Timothy D. Haugh:

So before I answer, how many people in the audience have served in a cyber operations or a cyber ISR unit at any time? This is why we're integrating more effectively. You see the number of people in this

room, the talent that we have, and that's been grown to be able to integrate. And what I think of when we think about how we're integrating with the other combat and commands... One of the three UCP missions of US Cyber Command is support to the other combat and commands. It starts with that talent.

In terms of our ability, the maturation of each of the service Cyber Component headquarters, the maturation of our integrated planning elements that are with each of the combat and commands and they are every day working to campaign to develop operations, investments, and to be able to have outcomes. Whether that's defensive outcomes and partnership with us strategic command to think about defense of our NC3, the partnership with US Transportation Command as we think about global logistics. With each of the geographic combat and commands that have challenges every day, that has really been advanced by the talent and our ability to plan and our ability to operate as we mature as a force.

So I think that really puts us in good stead as we go forward that the talent now has the authority to be applied and to be effective in campaigning with each of our partners.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Thank you. Now, when I was the TRANSCOM 6, we were very, very cognizant of the fact that a significant portion of the nation's lift, both air and maritime as well as the land lift and transportation, was in the hands of the private sector. And based on the fact that our military relies on critical infrastructure, both domestically as well as abroad, in its ability to execute its mission, cyber issues everywhere and critical infrastructure domestically and abroad are something that's front and center on the minds of our key senior leaders as well as many of you.

So as we take a look out of my organization, the CERT, we continue to see critical infrastructure as a target for cyber enabled tax, including things like denial of service, malicious software, ransomware, theft of intellectual property... We're very concerned about that, but there are some good news out there. And with the National Infrastructure Protection Plan, assigning lead departments and agencies to support those 16 critical infrastructures we have here in the United States. I'm kind of curious as to our panelists, what do you think and how do you think we're doing in coordinating across the inter-agency process to better manage the nation's cyber risk exposure? And we'll start with General Haugh.

Lt. Gen. Timothy D. Haugh:

So Greg, it's an important question. As we think about critical infrastructure at US Cyber Command and NSA, that has really started with election defense and the work that began in 2018 to be a partner in support of DHS and FBI to defend our elections and our electoral process. That foundation was really built on how we collaborated with both DHS and FBI, but also how we share information. And as US Cyber Command, we've received significant new authorities on how we can partner with industry and to share information directly. We will do that in concert with DHS and CISA and with FBI. But between Cyber Command and NSA, that ability to share information, to share in an unclassified level so that we can move with speed and agility, to make threats known and to make that very transparent, so that industry can act and ensure that they have the best set of knowledge to be able to respond if there is any sort of threat to our critical infrastructure.

Brig. Gen. Gregory Touhill, USAF (Ret.):

And that's crucial for the providers that are out there, not only in the large businesses, but also small and medium business and having access to information, showing what the threats are, what the risks could be, as well as what to do about it. Very critically important. And in the space domain, we've got great partnerships with many different critical infrastructure providers, including the

telecommunications providers, the defense industrial base and others. And now we also have a very burgeoning space industry. So how's things going in that realm as far as information sharing and what can we look for in the few years ahead, regarding information sharing on cyber issues in space?

Col. Zachary “Shay” Warakomski:

Yeah, I will tell you, even beyond cyber, if you go out to Vandenberg to our Combined Force Space Component Command, we have a cell that sits on the operational floor for the combined Space Operations Center there. And basically that's your nerve center for all things space 24/7, 365. And we have the tethers back to several industry partners that are, whether they're working satellite communications or imagery, a whole host of things. And it doesn't have to do with just space operations.

We are focused on... There's a cyber front there as well. I will tell you one of the efforts that we're working that my team is working in conjunction right now with Major General Gagnon at the service level. If you think about our installations, again... Because we fight from, we are employed in place and fight from those installations, we've got a concentric ring effort where we're looking at our mission system platforms... Think of the CROWS model and dealing with the PMOs from that standpoint to be able to secure all and eliminate the vulnerabilities from that standpoint. Bring it out just a little bit to the installation. Obviously we work very closely with General Kennedy's team at 16th Air Force as the Space Force is a customer of the Air Force network and certainly with Air Force IMSC.

And then even broader outside the gates if you will, we're dealing with, think of the utility companies for ICS/SCADA. Operational technology across the board. Those are the types of things that we're working so that we can lean on, not only IC in terms of Intel informed threats and operations that we're doing there, but think of Colorado Springs utilities, to be able to work with them to eliminate those single points of failure. They're absolutely critical to be able to project power into and from space.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Thank you. And you mentioned CROWS, which may be an acronym that some members of the audience don't know. Cyber Readiness of Weapons Systems, right? So as we take a look at a lot of our weapons systems that we have out there... Earlier today we talked about the need to continually recapitalize a lot of our systems and we have some of our weapons systems have gone through numerous block upgrades. But what we need to do, and the Air Force has really been leading on this, is make sure that the systems that we have in place are secure by design and making sure that our weapon systems are cyber ready and we continually make sure that they're adapted for the environment in which they're going to operate. So we have a team, Air Force Material Command is the lead for that. And the CROWS team make sure that those fielded systems, some of them are older, they have the right cyber protections to make them endure and fly, fight, and win, regardless of the environment. So just a professor grab on the undefined and perhaps unknown acronym of an organization that's really important.

So doctor, you're leaning in on this, you'd like to talk about inter-agency as well?

Dr. Wanda T. Jones-Heath:

Yes. And you mentioned CROWS, so let me throw another one at you. CROCS. So that is the Cyber Resiliency of our Control Systems. Right now within the Department of Air Force, we don't have one entity that is focused on our defense critical infrastructure control systems, ICS/SCADA. So we wanted to make sure that we have that organization and I'm pushing hard with the secretary to stand that up

because I realized after having a operational technology summit, there are about 10 offices within the DAF that have something to do with securing those DCI assets.

And let me take you back in time. 2018 was the first year that NDA, language 1650, where we had an opportunity to really look at the DCAs, our Defense Critical Assets and our TCAs, to be able to understand what it looks like, what do we need to do to secure it, and then how do we mitigate some of those risks. Right now we are in the midst of doing our first base of mitigating those risks. But you got to understand, we don't have enough money to fix everything. So the right investments, fixing the right vulnerabilities will go a long way. We have a long way to go as well. And we're trying to make sure that from a palming... planning and palming perspective, that we also add our DCI critical assets.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Well that planning, programming, and budgeting system arrears its head again there. One of the things I learned when I was the panel chair in the corporate structure was if it ain't funded, it ain't. Now we can talk about... Yeah, think about that one, right? It's on the coin for SAF FMB. As you take a look at the operational impacts of inter-agency, working across... the inter-agency in addition to the Joint and combined community, General Kennedy, what's your perspective on how we're doing in integrating that inter-agency aspects of defense of the nation?

Lt. Gen. Kevin B. Kennedy:

All right, thanks Greg. I was surprised when I took over a little over a year ago at 16th Air Force as an operational numbered Air Force commander of how much actual inter-agency coordination still has to continue, at that my level and previously as the director of operations at a combat and command and at Cyber Command. And that made sense. But at our level we have to have that level, whether it's locally in San Antonio to help assure our mission, which we've talked about, the dependence on the other critical infrastructure and sectors or whether it's as we're posturing cyber protection teams and forces to support our CONUS base combat and commands that are employed in place with TRANSCOM, with NORAD NORTHCOM, and with STRATCOM who rely heavily on US-based critical infrastructure to execute their mission, as well as mentioned by Shay, the Space Force employed in place model. And we have to think through that.

So how do we enable all that? It comes back to what General Haugh talked about at the beginning, information sharing and being able to do that with confidence that the information is going to be secure. So within the Air Force, we're being fairly aggressive from a base level to all the way up to NAF level to Air Staff level of trying to get to a better resiliency position and a better censoring position so we can understand what's going on within the United States Department of the Air Force as we're going forward on that.

Within our mission systems, as we mentioned CROWS and others, we're looking, okay, how can we understand the life cycle of information? And what I mean by that is as we're in a competition based environment, confidentiality, availability, integrity are in varying levels of importance and the availability may be slightly less in competition than I needed in crisis or conflict. And we have to be agile enough as we're going through to understand when I can accept risk in making it more available, but maybe less confidential as we're going forward. I would say we need integrity throughout, but that's encryption.

But as we're thinking through of this type of framework is really working closely with the mission owners and through CROWS and now CROCS as we go forward. And all I heard in Wanda's conversation, she's funding everything 16th Air Force is asking for. That's what I heard. And Ms. Goodwine's right here too. So you all heard it. There's about 2000 people that witnessed that. But that's kind of the focus at the operational level of where we are on how we do that. And that goes with our partners and allies as well.

The key in competition is information sharing. If they don't have secure environments, it's going to limit it.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Well thank you for that spoiler alert as to what's on the top of your Christmas wishlist. No, thank you very much, sir, for that. Now I'm going to quick do another audience poll. How many of you maintain a certification from a organization such as ISAC or (ISC)², CompTIA, any cyber operators out there have a CISSP, CISM security plus or whatever? Okay, a significant number. All right.

Now like many of you and many military cyber professionals around the world, I maintain my professional certifications with my CISSP and my CISM and we're seeing that in the industry and I'm on the board of directors of ISACA. So during COVID, we actually saw a huge jump in membership as well as the demand for certifications. Now we're in a competition for manpower and personnel. Like any business around the world, getting the right talent and competing for that talent is a challenge. The most recent (ISC)² annual workforce study saw a 5.5% increase in the US cyber workforce. Woo-hoo. But you know what? The demand signal continued to go up and we now have a job vacancy rate here in the United States about 8.5% according to (ISC)².

So given the fact that we are looking for really great talent and folks with great potential, we've got to compete for that talent and mission goes a long way. When I raised my hand on September 6th, 1979, we were still mainframing. Now everybody is a cyber user, a cyber operator... And Major, thank you for laughing at the reference of 1979. Yeah, I appreciate that. So given all of this, we're going to start with Dr. Jones-Heath.

Doctor, how well do you think our Air and Space Forces are competing for and retaining these high demand, low density personnel in today's dynamic and very competitive marketplace? How can we improve?

Dr. Wanda T. Jones-Heath:

So thank you for that. The workforce is certainly important. I like to title this the Race for Talent. We are all trying to find the right skills and the right folks for the right jobs. We're competing against each other, service wise, as well as with the COCOMs and industry. So we have to find a way to work together. Ways where we can exchange talent from industry into the services and vice versa. So we have to think differently. We have to take some risk. Our hiring practices... It takes a long time to hire a civilian. How can we fix that? It's a process. Working with our personnel community to be able to streamline that process, because you offer a tentative offer and then it takes seven, eight months. That person is gone and that might be the very person you need for your team.

We're starting to really engage with the cyber workforce approach, looking at the codes that we need to make sure that we are finding that right talent. Understanding what we look like, that's part of it. Knowing what you already have and then capitalizing on that, making sure that if we're looking for cloud architects and we have them somewhere in the services, how do we get them in the right jobs doing that? And so we need to do a lot of that.

We do have a opportunity to use hiring authorities, taking advantage of all those things that Congress has already given us. We don't do enough of that. Using different types of pay structures, CES as one of the options. We have a lot of things that we can do, but we have to take risk. We have to be bold and that's what I want to see in the future.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Thank you. Let me reach over to the Colonel because thinking differently spurred the creation of the Space Force. How is Space Force thinking differently in recruiting and retaining cyber workforce?

Col. Zachary “Shay” Warakomski:

So first and foremost, as the smallest service, any loss across the board can be extremely impactful, just given the sheer numbers across the board. I will tell you though, that we have partnered with the Air Force a DAF Initiative across to be able to get after the retainment.

We're never going to be able to pay our Airmen and our Guardians what they're going to be able to get on the outside. There always has to be a sense of service, a sense of patriotism, certainly with regard to this. However, we are working right now, there's selective reenlistment bonuses up to the 14 year mark. We're also doing the special duty assignment pay for those once they complete their initial skills training. And then there's also a cyber assignment incentive pay that's out there as well. So this kind of this trifecta, in particular for us, for our cyber operators to be able to do everything that we can within the limits of the law to be able to keep them, to retain them, as long as possible.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Well, you just said something that reminded me that no Airmen or Guardian, soldier, sailor, marine, or Coast Guardsman joins up to make money. They join to make a difference. And as we as Airmen and Guardians try to make a difference, making sure that we have the people on either side of us to help execute that mission is really important. General Kennedy, I pose that same question to you as the operational commander, how are you viewing us and the retain and the recruiting?

Lt. Gen. Kevin B. Kennedy:

All right, thanks Greg. I just kind of doubled down on the comments Shay had is at 16th Air Force and within our units we look to create a culture that's founded on our core values, service, integrity and excellence, and a culture that we hold each other responsible and accountable to those with a level of self-discipline. I think that's what attracts folks to national service is we want to serve that are cause greater than ourselves and we want to serve with like-minded Americans that are also oriented and we want to serve in a place in an organization that holds each other accountable to these values. So that's the first thing that we look to do.

Now the second one is, I also agree with Shay is every Airman that I can retain once we have them in the force is a win. One. One Airman if I can retain them in the force. Now the question is where in the force, if you think about the three by three matrix that we have, we have enlisted officer civilian, we have guard reserve, active duty, and we're thinking of how we can be more portable, how we can be more collaborative across those different components to enable service where the Airmen has responsibilities that might make active duty service something that they can no longer sustain, based on some other commitments in their lives, want to retain them in their participation as they can in our environment, whether that's as a civilian or whether that's in a different component.

So Congress has given us a lot of very flexible authorities where we work with Dr. Jones-Heath and Ms. Goodwine and the A26 and General Lauderback's team to figure out how can we get these in position to get even just one Airman retained as we're going forward. So that's really our focus as we're moving forward from 16th Air Force

Brig. Gen. Gregory Touhill, USAF (Ret.):

General Haugh, from the Joint community, sir.

Lt. Gen. Timothy D. Haugh:

We may not have enough time because I've really, this is our number one issue. This is the most important thing that we'll talk about today. It's about our people. And so I'll touch on a couple of things really quickly about our culture, our authorities, and then the advocacy that we can do from US Cyber Command.

Everybody talked about culture. As US Cyber Command... As really a growing combat and command, we've existed for five years as unified combat and command... General Nakasone spent time over the last year saying we need to set our culture. The number one thing that when we did that and when really our senior enlisted team did that work and came back and made recommendations, it starts with we win with people. We have to partner, we have to empower and we have to deliver. And we've got to be able to let everybody see where their service and how it impacts.

And we can do that in any number of ways. We think about the authorities that have now been given to General Nakasone that when the budget passes for FY24, he will now have enhanced budget control, meaning the responsibility to execute the entire department's budget for the Cyber Mission Force and where is he initially invested that budget? Back into our people and into our readiness. Our training environments, our ranges, our ability to integrate our garden reserve in a way that allows them to enhance currency.

And then our advocacy. As US Cyber Command, underneath the unified command plan, there are a number of sets of authorities that the President has given to General Nakasone and the Congress. And one of those is to evaluate the services readiness, the ability to retain, the ability to promote and to be able to communicate back to the department the strength and health of the cyberspace workforce. We're seeing a number of really good things across the services. The Army has done some really unique things in terms of how they've done early promotion and their incentives. The Marine Corps has actually added billets to our cyber Mission force teams, so it fits better into how they intend to leverage their talent both within the fleet and in support of US Cyber Command. We've talked about a number of things the Air Force is doing.

What we're advocating for in US Cyber Command is more commonality across the services to leverage those areas that we see successful within each of the services as opportunity to be able to employ the entire force and retain greater numbers because the talent. We win with people.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Thank you, sir. My last question and we... I am sensitive to the time. It's a organized training and equip focused one, so service reps start feeling uncomfortable. It's coming your way.

So one thing that when we talk about cyber workforce, there's a lot of good lessons out there from industry and Steve Jobs reportedly said... I didn't actually witness him, so it's only a report. Jobs is quoted as saying technology is nothing. What's important is that you have faith in people, that they're basically good and smart and if you give them the tools, they'll do wonderful things with them.

So given that, I would like to pose to the Colonel first and then to General Kennedy, do we have the right tools for cyber workforce? What can industry do better to help our Airmen, our Guardians, our soldiers, sailors, marines and Coast Guardsmen, what can we do better from an industry standpoint to help them execute their missions better in defending our country? Colonel?

Col. Zachary “Shay” Warakomski:

So to take a page from the acquisition community, we have to exploit what we have, buy what we can, and only build what we must. In that vein, we have to leverage industry to the max extent possible. I

think we've done that pretty well on the Space Force side in terms of the DCO suite, Manticore, Kraken, that we're developing today. We've basically taken commercial off the shelf hardware and software and we're rolling in an agile DevSecOps environment to be able to tailor that to the particular mission system enclaves where we maintain a persistent presence to be able to put that kit down and those operators to be able to operate day in and day out.

And so where can industry help us? It's all about integration and automation at this point in particular. The automation, anything that we can do to erase mundane types of activities for our Guardians and our Airmen across the board, you should be all over that, hopefully. Integration as we deal with antiquated platforms that are decades upon decades old to be able to integrate in that new environment is sometimes often very difficult. And so that is where we could certainly leverage your skills and expertise.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Thank you. General Kennedy.

Lt. Gen. Kevin B. Kennedy:

All right, I got 16 plus 10 seconds left. So what I would offer is technology isn't everything, but I would say Airmen with technological depth is everything. And I need Airmen that are trained so that they can maintain the pace of change that shapes our domain. What can industry do to help? Any capability or tool that you bring to us, bring training, make it modular, make it self-paced, but also have mentorship options.

Brig. Gen. Gregory Touhill, USAF (Ret.):

Complexity is the bane of our adversaries, but simplicity is the archnemesis of our foes. So keep it simple. Make things secure by design and secure by default. And to thank our panel, I had like to say thank you for your leadership. Thank you for your vision. Thank you for your stamina as you continue to serve our great country. And thank you for joining us today.

Lt. Gen. Kevin B. Kennedy:

Thanks, Greg.