Maj. Gen. John Olson:

Okay. Well, good morning. It is a pleasure and honor to have you. I'm Major General John Olson, and I am the chief of space operations' mobilization assistant for General Saltzman in the Space Force. I also lead our combined Joint All-Domain Command and Control, as well as the Advanced Battle Management System in C3BM. It is a pleasure to have you with us for this panel, which is ongoing to be Space Order of Battle. This is the second one of the AFA event here. I'd like to congratulate you upfront because you are the hardcore, interested disciples of resilient space power, because I know we have some pretty stiff competition with Admiral Grady as Vice Chairman of the Joint Chiefs next door. I'd like to give yourselves all an applause for being the hardcore ones.

We are super excited. We've got a great lineup for you. As I mentioned, this is the second of two panels. I think that just underscores the critical importance of this time, this moment, this place in history where we are transforming to rise to meet the challenges of the threat of a congested, contested domain, a space warfighting domain. As we look forward to that, I'd just like to say upfront, thank you to AFA for having such a great set of panelists. I think this is an indication of the critical importance of this. Much like that first panel had some outstanding results ... I encourage you to look online at that. I was unable to attend it in person, but just listened to it and I found it to be very catalytic. You'll find that we'll weave in those messages here as well.

Much like Top Gun ... The original movie was awesome. It would have been even better had that been Air Force in there, but we'll give them a little bit of license there. Much like the second follow-on, Top Gun: Maverick, was even more awesome, I expect ... And that's laying the bar out right out now for this panel, so we're looking to bring it strong. As we talk today, what I'll do is, first, introduce our panelists. Then I'm going to set the scene for you. Then they'll do some self-introduction and we'll give them each a summary moment to get across the key synopsis, the key, primary threats, and then we've got some riveting questions. Because you are the hardcore disciples, the ones who chose to be here, we're going to also see if maybe we can open it up to your riveting, hardcore questions, and we'll do some lightening rounds here at the end, so I think it's going to be a great setup.

On the panel today, so we've got Mr. Stephen, Steve Mare. He's the vice president of missions and campaigns for Space and Intelligence Systems at General Dynamics Mission Systems. Likewise, we've got Mr. James, Jim Reynolds. He's the vice president of business development for Defense Space at SAIC. Then, of course, we've got Mr. Scott Stapp. He is also a brigadier general, Air Force, retired. He is the chief technology officer for Northrop Grumman. I think building on their 25-bound brains each, this is going to be a catalytic event and really going to be exciting.

Without further ado, we'll go ahead and we'll set the scene-setter here for you. As we know, deep into the 21st century here, space resilience, or a resilient space architecture plus partnerships, and particularly partnering with industry, this is how we're going to drive dominance. Now, are we going to have temporal dominance here or is this going to be sustained? I think that's going to be a debate, something that we'll be talking about.

As we look at it, of course, the chief of space operations rolled out our brand new Space Force mission statement, which is to secure our nation's interests in, from, and to space. We're doing that with three lines of effort. The first line of effort is to field capable, ready, combat forces. Now, of course, with the theory of success that underpins a competitive endurance, we don't want to have to fight in space, but that's not our decision. Our adversaries have already been fielding both kinetic and non-kinetic, and multivariate threats to the environment from both in space as well as the ground and the air.

As we look at that, the second primary line of effort is to amplify our Guardian spirit to drive those core values of courage, character, commitment, and connection. To amplify those, because as we all know, people really are at the core of any mission's success. Finally, which is really appropriate for today, it's partnering to win. Partnering to win, yes, with industry and evermore, the Space Force is born digital and lean by design.

Those partnerships, and these are three fantastic exemplars of that, from an industry side are so key, but also international, interagency, the institutional side, and of course, academia. I'll give a shout-out. We've got the Honorable Heather Wilson in the front here. As former Secretary, when we tie in the academia side, that is so important, both from a people pipeline, as well as an innovative concepts, and ideas, and experimentation. Those relationships are absolutely so important. That's how we're getting after that mission, but it is congested and contested, and this is just a snapshot.

We're being threat-informed and threat-driven because as we look at our adversaries and competitors out there in a great power competition, hundreds of satellites already are at play by our competitors and adversaries, and so this is a challenging environment. For that, the Secretary rolled out the seven operational imperatives, plus her enablers. Those are very important, but the first one, operational imperative one, and I emphasize the operational aspect, that as the Space Op lead for our CJADC2 activities, that's a resilient space order of battle, fundamentally important, first, upfront because all the Joint Service and Coalition activities depend on it.

Secondly, OI two, operational imperative two is operationally optimize CJADC2, ABMS, and C3BM. That is the OV-1, SV-1 that overlays all of this, and so very, very important. Then finally, when we talk about moving target engagement with OI three, MTI is fundamentally going to be enabled. When we have the tyranny of distance and the first and second island chain challenges, space is going to be a huge enabler. The common thread of the OIs is the first three are really space-centric. When we talk about a space order of battle, I think that really sets the context for today's talks. To drive this resilient space order of battle, it is threat-informed. It is outcomes based, and mission-driven.

We know that protect and defend is a core part of our mission ethos, but we need to have a sense of urgency, a sense of agility, a sense of ... A step-functioning increase in the rate and pace here. This applies across not just the space segment, but all four segments. The ground, user, launch, and space segment. As we drive towards that, again, focused on operational responsive capabilities, I think getting to the fundamentals or building off of a foundation that's built just like the three Rs for reading, writing, and arithmetic, certainly, resilient, robust, and responsive are the attributes that must characterize our space order of battle.

As the Secretary has said, the answer to China, China, China is space, space, space. With that, I would like to absolutely say this is how we're getting after it. Space domain ... Pardon me. The Space Development Agency is driving our Proliferated Warfighter Space Architecture. Our Space Warfighting Analysis Center is driving a model-based, threat-informed force design effort. This is at the heart of everything that we're doing.

As General Saltzman says, it's all done through a campaign approach. We drive a theory of success based upon competitive endurance by having a comprehensive and deliberate budget and personnel requirements process that also is exercise, because training people, tactics, techniques, procedures are at the core of our mission's success, and we got to do that all at the speed of need. That is the opener from which we are going to launch into a really exciting panel, so over to you. First, we'll have Mr. Scott Stapp. Go ahead and introduce yourself, and give your summary overview.

Brig. Gen. Scott Stapp, USAF (Ret.):

Okay. Scott Stapp, Northrop Grumman. I actually came out of the corporate CTO job, and now I get to do the fun job of, actually, I run what we call our corporate campaigns for JADC2 and National Security Space. If you've talked to Luke Cropsey, that's my job, trying to integrate everything. It's one of those world hunger kind of jobs. My background, I'm actually a 30-year Air Force guy. I'm the guy in the Air

Force that they forgot about because of my 30 years. I did 20 joint or interagency, to include three Joint Staff tours, one in the vice chairman's office, and one running the JROC, and then finishing up as the OSD, SAPCO.

As we talk about this problem set, you're going to get, at least from me, a very purple look at how you look at some of this. The other is really just looking at the interagency. I was also the director of what is now SAO over at the NRO, so when you start to look at space, when I was out at the NRO is when you couldn't say NRO. I mean, everything was black. You can't talk about it, you can't do anything.

What I think we're going to see when we start talking space order of battle is you cannot run everything in the black. You actually have to start being able to talk it. There is no warfighting demand we have, air, land, or sea that you don't talk about all the stuff you do. They have to be able to operationally plan. They have to be able to integrate, and they have to actually be able to ensure that the elements they have are getting tied together. You cannot integrate things that you don't know about. As we go forward, that will be one of the big themes, I think, as we look at what does that space order of battle really look like.

Maj. Gen. John Olson:

Excellent. Next up, we'll have Jim Reynolds from SAIC.

James Reynolds:

Thank you, General Olson. Yeah, so Jim Reynolds. I work at SAIC, and I work the business development or the solutioning for our defense space account, which is really all the capabilities, all the support we provide to the Space Force. My focus there is really on multi-mission integration, rapid delivery of mission capabilities to really address the challenges of joint warfighting and the integrated battle space. Prior to that, I retired from the Air Force in 2019.

I had a career that was mostly in space, mixed between acquisition and operations, and worked a lot with the National Reconnaissance Office here in D.C. and the Pentagon, and then finished up my career out in Los Angeles at Space and Missile Systems Center, which is now Space Systems Command, and so the culmination of my career. It's really an honor to have Secretary Wilson and General J.T. Thompson in the audience here. Was working for them and supporting the foundational elements of the Space Force, the organizational elements, the policy elements, the budgeting and requirements that had to be aligned or realigned to really address the challenges of joint warfighting through, and as the new Space Force mission statement states, through and to space. It's an honor to be here today.

Maj. Gen. John Olson:

Excellent, great. Now, last but certainly not least, Steve Mare from General Dynamics Mission Systems.

Dr. Stephen Mare:

Thank you, General. I'm Steve Mare from General Dynamics. I lead a business unit that has a space command and control business, and like Scott, I also lead a campaign for GD's JADC2 efforts. I've been, like Jim, both a space operator and a space acquisition guy for my 21 years serving in the Air Force. I'm hoping to be a legacy Guardian in the not too distant future.

In the 30-plus years that I've been involved both on the industry side and government, I've never been more excited about this particular topic because we're right at that cusp where we've gone from the point where, largely, space provided services, and we're now openly talking about space as a warfighting domain. For the Guardians in the room, and their industry counterparts, and Airmen as well, getting this right over the next three to 10 years and setting this service up for long-term success in the space order battle is critical, and just happy to be able to support. Thank you, sir.

Maj. Gen. John Olson:

Okay, great. I would like to launch into some pretty compelling questions. We're going to make this a little bit of edutainment. We're going to make it dynamic. We're going to be a little provocative, but I think the unvarnished inputs will be fantastic. Again, be thinking of some questions that you may have as well and we'll see if we can facilitate those at the end. First off, Scott, the space order of battle for OI or operational imperative one focuses on increasing the resilience of space assets in the face of increasing threats. What will drive greater resilience and more robust capabilities in today's space architectures, from your perspective?

Brig. Gen. Scott Stapp, USAF (Ret.):

I think we have to take lessons learned from the other domains. When you talk resilience, I don't think there is any one-size-fits-all when it comes to resilience. I think you have to actually look at multi-orbital regimes, LEO, MEO, GEO, HEO. You have to look at how you proliferate so you have larger numbers. That builds resiliency, but I think one of the most important things is everything has to be networked together. When you start building ... I mean, if you look at the IT world today, if you take out a single server somewhere, basically, all the information just reroutes through everything else that's available. All the systems need to be interconnected. Data needs to flow across the entire ecosystem, and this gets back to this whole discussion on if everything is working in the black world ... Again, my last job, OSD, SAPCO is nothing moves fast when it's in the black world. Everything is stovepiped. Nothing interconnects.

If we are going to actually make space a warfighting domain, everything needs to know about everything else. They all need to connect together. When one thing gets taken out, it is not the end of the world. It just reroutes and connects to everything else that's available. When you have disaggregated architectures, you have much more availability. We've seen the Space Force and they're moving to this, which is sustained maneuver, which is really interesting because that is really an Army doctrine activity, which is if you are static on the battlefield, you are going to die. Well, they're starting to learn that in space, that even though it's not static, it is relatively static and moving sustained maneuver, which means you got to get into logistics.

It is really building up an entire ecosystem that actually builds in resilience across the board. I think there's a lot of lessons learned from what we've done in the other domains to actually build that into it. We are just at the very beginning. Space has always been this peaceful domain that nobody was supposed to be fighting a war in, and it was also always, when it came to DoD, in the black world. It has got to come out of that world and it's got to operate like the other domains.

Maj. Gen. John Olson:

I think you nailed it on the network capabilities, the multi-orbitalogy, the security built-in as an essential element upfront. Of course, Lieutenant General John Shaw and the team, as we have rapidly advanced the concept of sustained maneuver in dynamic space operations, I think these are all great attributes. How about Steve and Jim? You got any further thoughts on what that means, or any additional attributes or characteristics, building on Scott's thoughts on that?

Dr. Stephen Mare:

Go ahead first.

James Reynolds:

Okay. Certainly, I don't really have a whole lot more to add, but it's the interconnection of myriad of capabilities. It's that how do you bring the data that's coming off of these systems to bear for decision-making in a rapid fashion to close those kill chains?

Maj. Gen. John Olson:

Yeah. We've heard in other panels, data, data, data is so core and centric, and it's not data for data's sake. It's data to drive information advantage and decision advantage at the speed of need and relevance. Anything else further?

Dr. Stephen Mare:

Yeah. I agree with everything that Scott said, but I think there's more discussion to be had. I'm going to break this down into two separate groups, assets that are currently on orbit and assets that we're currently building. For the assets that are currently on-orbit, there are things that could be done, need to be done by the Guardians and the industry partners in terms of how do we protect those systems. Just because they're on-orbit doesn't mean that we can't do things.

For example, in the TTPs, are we practicing if when attacked and we have degraded power on the satellite, what are we going to do? We need to get to an operate through mentality as a force. The other thing is, and I know Scott's company is working on it, in terms of just because the satellite's in space doesn't mean we can't add capability to the satellite through on-orbit servicing. So those are those on-orbit. In terms of the resiliency for things that we're putting into development, part of it is the just going to different orbits, adding quantity, but the other resiliency has to be throughout the entire ground and supply chain. All of those things have to be on the table when we talk about resiliency and how we're going to do the order of battle.

Maj. Gen. John Olson:

I think you hit some really important points there. Certainly, the ground segment, the industrial base. Not just the space industrial base, the much broader industrial base, both of the United States, and our partners, and coalition allies, supply chain. As well as, of course, when we talk about ISAM, the U.S. national policy on In-Space Servicing, Assembly, and Manufacturing. SAML is part of the spacepower doctrine, which is space access, mobility, and launch, which also includes logistics. I think those are great, and I think really helps characterize and puts some meat around what we mean by a resilient space order of battle.

Second question here is going to be, Jim, for you, leading off. How can industry and government best collaborate in building the architectures necessary to be adaptive and effective in thwarting threats to our space systems in the future? We talked about today in the previous question. Specifically, what are you top three priority recommendations? Just as foreshadowing, be thinking about yours, Scott and Steve.

James Reynolds:

Great. Okay, yeah. Thanks. First I just want to ... When you talk about government and industry as kind of monolithic elements, it's really a lot of different elements to each of those. With government, you have your policymakers. You have your force design analysis. You have the requirements, the budgeting, the acquisition, the operations, training, testing. All of those groups have to be able to collaborate together. Then similarly, with industry, you've got developers. You've got advisors, consultants. You've got small business. You've got commercial and nontraditional that we're all trying to bring to bear.

I think the most important thing we can do is establish a collaborative environment for all of these groups to work in. That has to be done to not only protect information from a national security perspective, but also from an intellectual property perspective in order to get all these entities to work together, and then be able to visualize the information in a way that makes sense to them so they can use that to make decisions. Whether it's an operational view, an architectural view, a performance view, cost or schedule analysis view, how do you bring that all together?

Having that, and getting back to the question, if we can establish that environment, then I think the top three priorities on what to use that environment to do would be, one, to do the kill chain or the kill web analysis integration. That's really where it all comes together in determining your gaps, your threats, being able to identify the priorities that we need to work together to close, and making sure we can close those gaps in the right timelines. From integrating your data, your sensing information, to being able to visualize and organize that data for decision-making and then finally, for fire control, being able to actually generate effects in a timely manner to close those kill chains.

The second piece of that, second priority would be an interconnected battle space. To do fire control, it's not going to be just space that's doing that fire control. It's going to be all elements, multi-domain integration in a resilient and cyber-protected manner because that's where our adversaries are going to go after and break down the threat.

Then lastly, the last priority is being able to accelerate capability delivery and integrate that capability directly into operations in a continuous manner to address threats as they evolve and they change, to address technology improvements as they present themselves. That's really the culmination of it all. The way that we can achieve that last priority, I think, is right now, most of our interaction between government and industry is through two means. One would be your traditional development contracts, where industry is contracted to provide a specific system, a specific capability, typically. That's how we budget. That's how we set requirements.

Then we also have a set of contracts for augmenting the government workforce through consulting, SEDA, A&AS, FFRDC support. What we don't have a lot of are multi-mission integration contracts with deliverables for delivering integrated capabilities. That's where I see a priority for government and industry interaction would be in establishing those working relationships, those contracts so that we can continuously integrate, continuously deliver capabilities into operations, go through your testing, your training, your ops acceptance, the accreditation in an agile manner. If you don't do it that way, you have to do everything agile or you don't do anything agile.

Maj. Gen. John Olson:

I couldn't agree more. You had some really excellent points in there. One of the mechanisms that the Space Force has enabled is leveraging the COMSO, which is the Commercial Space Office out of Space Systems Command, and we also recently opened an office called COSMIC in Chantilly. Those are just two of the mechanisms, but we're trying to really improve that integrative and that back and forth between industry and the government. I think there's a lot more. Certainly also, in a CJADC2 or a C3BM perspective, as we build out the DAF network, having an integral relationship with industry to that is so very important.

We rolled out the model-based systems engineering model just here on the 11th, and that's going to be an ongoing approach to developing and refining the operational requirements, which then in turn gets translated into the systems assistance architecture as well as the acquisition element, so we can pull from that. We have over 200 industry vendors and providers on that IDIQ, and I think that's going to be critical, but I think there's a lot more that we can do. Any thoughts on that, Steve or Scott?

Dr. Stephen Mare:

Let me start off by talking about things that I think we're doing right. One of the things that has been done consistently over the lat 10-plus years is good dialog from the government to industry on the threats. We get together in the right security environments and we talk about the threats. I think that's a good thing. We would, of course, love to do it more. We're always interested in how the threat is evolving.

The second thing is the work that's being done in the SWAC. What I think is going to happen over the next decade is that not only is the threat going to involve the technology, and so we were having this conversation with one of the GOs yesterday that, as these things start to happen, as we start to refresh these architectures, there are going to be times and places where we want to have an open and honest dialog about, what are new ideas? What are better ideas? How do we do this? One of the things between the government and industry is we need sort of a sandbox with the right security levels to try out ideas on a low-cost basis to try to weed out the really bad ones and then invest limited dollars in the few good ones that remain. I think that's probably the biggest thing.

Maj. Gen. John Olson:

Scott?

Brig. Gen. Scott Stapp, USAF (Ret.):

Okay. I'm going to think of it slightly different. I don't think any of this is a technology problem. I think technology exists today to solve most of these problems, and I will oversimplify. When I look at space order battle, there's two things it needs to do. It needs to support the warfight from space, and it needs to support the warfight in space. Those are the two basic elements. When you look at supporting the warfight from space, literally, up to now, which is when you start to look at a DoD construct, which is really this find, fix, track, target, engage, assess, F2T2EA, all ISR is done by Title 50. Their job is intelligence. It is not warfighting, so this doesn't get into a technology problem because the technology exists. This gets into a, how do you integrate everybody together?

Some experience from the JROC. We used to call ... When we'd bring folks in, the joint community was more about joint deconfliction than it was joint integration. We did not do ... Look at F-35. We used to have debates on how may Gs, different service aircraft had to pull, and in the end, we'd go, "Well, if you only pull seven Gs in the Marine Corps and you pull nine Gs in the Air Force, do one guys die in larger droves?" The answer is no. What you get to is, we coined a phrase, was “desirements.” Everybody wants their own thing, so if we're going to start working in a community and space ... Again, supporting the warfight from space now involves the Navy, the Air Force, the Army. It involves everybody else. You cannot drive your own desirements.

It truly now has to be an integrated approach, so when we start talking about government and industry, there needs to be a better government integration. Then, the government as a whole has typically been very one-on-one. We, as a whole, tend to build widgets. We build platforms that do very specific missions. We build requirements around those missions, but the idea that those platforms actually work and integrate with every other platform around them, that has not been a thing, so getting from system requirements to system of systems requirements, which means you have to think much bigger picture. That means that the folks in industry now need to integrate and be in, basically, more consortium-type activities.

Those who've been involved in consortiums, they are unbelievably painful from an industry perspective because you're always fighting, but they're unbelievably productive. They actually come up with solutions. What we need, really, is a consortium that does industry, which we're used to, but government consortiums, which have multiple different government agencies actually having to be on the same consortium so they have to fight out those same requirements amongst each other, both DoD and the IC. I think we're going to have to work through some of these policy issues between Title 10, Title 50, amongst the services and what they can do so that you come up with more integrated requirements and not agency or service-specific requirements.

Maj. Gen. John Olson:

Amen. The Partnership Integration Council, or the PIC as it's commonly referred to, does some of that bringing together the operations and the acquisition, bringing together the intelligence community plus the warfighting community, so I think that's exactly right. As we look at the Joint Requirements Oversight Council, JROC, on the 02921, it says, hey, the Space Force has the lead responsibility for the space requirements for all of the joint services, so you got to cooperate to graduate here. Really excellent comments. We're going to shift gears into the final question.

Steve, we'll have you lead off. Cybersecurity and data. They're essential and foundational to our systems of systems success, but I'm concerned about our integrated readiness there. What are you biggest concerns, challenges, and issues, and how can industry and government best collaborate to address these in a timely and responsive manner?

Dr. Stephen Mare:

I think there are two problems I want to talk about. One of them is synchronizing the enterprise, and the other one ... Well, let me talk about the synchronizing the enterprise. You have three different industry partners up here. We're all working on things that do cybersecurity functions like root of trust. We're all going to build, as Scott said, widgets, and then those systems will not operate holistically as a system of systems together. Why? Because there are no standards for how those are going to interoperate, so for the poor Airmen and Guardians that are going to have to figure out, when a threat arises and, "How I'm going to operate this in a battle management network standpoint," we're just creating problems down the road. The good thing about that is, as Scott mentioned, consortiums are a great way, although they're painful for us, collectively, to get after that problem. Let me turn it over to Scott or Jim.

Brig. Gen. Scott Stapp, USAF (Ret.):

No, I agree. Cybersecurity, what's interesting is it's we tend to think we're more secure on cybersecurity if you only have one device hooked to anything, whether it's a system or a network. Actually, again, this is coming from my experience at OSD, SAPCO, is you're actually more vulnerable. You have thousands of surfaces on which an adversary can attack you, and he's eventually going to get into one. Now, granted, when you hook everything together, you are much more vulnerable if somebody does get in, but with all the advances in AIML ... We used to do network monitoring, and if you look at all the things, the wonderful things, interesting things you can do in ChatGPT and others, when you look at anomalous behaviors on a network, that is where AIML just does amazing things, so you can start tracking down that anomalous behavior.

We're at this crossroads where nobody wants to hook everything together for fear that you run into this huge cybersecurity issue that once somebody's in, they're going to own you, but you can't fight the fight without tying everything together. I think there's going to be this tension between these two things for a while, but I think zero trust and AIML are going to actually get us a long way there.

Dr. Stephen Mare:

Yeah. Scott, you actually hit upon my second point. I think the way that the Space Force, in particular, is thinking about the problem ... Historically, we've always defended at the edge. I think the assumption now is you have to assume the bad guy's inside the network, so we need to have requirements that even on the satellite itself, does the main processor trust the sensor? Do we trust the command and control links? Because as Scott talked about, attack surfaces, I talked about supply chain earlier. You can have dormant attacks laid in the system that are turned on years after they're put in into the system. Those are the kinds of things the Guardians, and the problems they're going to have to work through.

They have to start thinking about the problem differently because again, the way that we're going to operate and the way the order of battle's going to work, it's going to require for us, over the vast distances of the Pacific, to work multi-domain. Therefore, we're going to have to hook things together, so we have to do it in a cyber secure way. It's got to become more to the fore of people's thought processes, rather than just worrying about the widgets.

James Reynolds:

Yeah. I'd add two things to that, so just building off what Steve's talking about. We have to not only start early from an operational perspective, but start early from a capability, development perspective, and really think about how we decouple our hardware and our software. Because right now, I think most of the time, we do cyber testing after the fact, system by system, and that really doesn't accurately portray our cyber resilience as an architecture or as a warfighting domain, as an integrated battle space. If you decouple the hardware from the software, the hardware becomes more foundational. It's something that you don't have to recapitalize as often. It's a bit more of a commodity, and you can establish a cyber position there, and then your software is what's continuously tested, continuously evaluated, continuously upgraded to overcome cyber threats, or improve capabilities if you can get into more of those cycles.

Then the second part that Scott was referring to, I think, that really, the ability to close the kill chain comes down to trust in our interaction between system-to-system or machine-to-machine interaction. There's going to be very little time for a person in the loop to be able to make decisions in time to then issue the fire control commands that are needed to defeat those threats, especially in a hypersonic missile threat, or those types of very short kill chain decision-making events where you have to really rely on the interconnectivity of your systems. Many of them are going to be in space, without the time that it takes for a man in the loop to be able to evaluate and make those decisions, and that's the trust.

Maj. Gen. John Olson:

Amen. It's core trust, DevSecOp approach, zero trust, ICAM, cloud, data, responsible AI, ML/DL, all of it. Great stuff. We're going to enter the final round here, lightening round. I would like to ... What are you and your team specifically going to do to drive huge outcomes or leaps in this arena as we drive towards a resilient space order of battle? 30 seconds each. Lightening round.

Brig. Gen. Scott Stapp, USAF (Ret.):

Okay. For us, it's nice to be a big company like Northrop Grumman because we build satellite systems, and airplanes, and weapons, and maritime systems. One of the things we've told the DoD, because it is very difficult to get the services and the IC all playing together is, we along with some of our other industry partners who are planning this, we're going to integrate all of our own stuff. If I integrate everything I have in Northrop Grumman, I have by definition, integrated the services and the IC, and I can do that internally, and they may get it as a freebie.

We're staring to work back with the government of taking everything we look at and no longer building unitary functions. Well, they'll still do their functions, but starting to develop an ecosystem where all the things will actually work together. If our other industry partners do the same thing, all that government has to do is integrate us together.

Maj. Gen. John Olson:

Jim.

James Reynolds:

Yeah, so at SAIC, I think we're traditionally, especially with space work, known as consultants or technical advisors to the government and we've been able to establish really deep subject matter expertise, really deep model-based systems engineering, process expertise. We've been able to also mature in other parts of our company. The digital engineering infrastructure, the collaborative infrastructure to be an agnostic integrator. We're not developing any of these multi-mission elements, so I think we can be an honest broker in collaborating across industry and government to create that environment that allows continuous integration, continuous delivery of capability.

We started some of that work with cloud-based command and control with the ABMS consortium. We're doing, with Space Development Agency, the BMC3 application factory, which is establishing this foundation so that you can bring in capabilities rapidly and integrate them into operations, go through the testing, get through the training, the ops acceptance, the accreditation so that every small business or commercial entity doesn't have to go through that cycle themselves. It really lowers the barrier to entry. It eliminates a lot of the burden that it takes to rapidly deliver capabilities.

Maj. Gen. John Olson:

Final word, Steve.

Dr. Stephen Mare:

Ditto to what Scott and Jim just said because we're doing all that too. As GD, because we're tier-two, we provide boxes, payloads, avionics to primes like Northrop Grumman. We do all that, but some of the unique things that we're trying to do is handle the multilevel security problem, which is tremendous in space. We're working on things that allow us to collect, or have different sensors on satellites operating at different security levels, bring that all down together, send that data to the right person at the right security level. That's going to be a big thing, especially when we get into coalition warfare, the fact that we can do. The other thing we're working on is edge processing. A lot of the satellite systems that are going to be filled in over the next decade, to talk about the timeliness that Jim talked about, we'll have to a lot of the processing at the edge, and so we're working in those technologies as well.

Maj. Gen. John Olson:

With that, that's a wrap. Thank you very much. We look forward to a continuing dialog with your engagement. All right.