FEDERAL NEWS NETWORK

STRATEGIC GUIDANCE SURVEY

Perspectives in Air Force: EITaaS

Brought to you by

AT&T

The Air Force's approach to its major transformation under the Enterprise IT-as-a-Service program may sound familiar to many long-time observers of federal IT.

Before the Air Force called it EITaaS, it may have been known as seat management or alternative service providers. The Department of the Navy has been on this managed service path for the better part of two decades with its Navy-Marine Corps Intranet (NMCI), now managed under its Next Generation Enterprise Network (NGEN) contract.

What's different with the Air Force isn't just the name, but the technologies, acquisition and collaboration models that underpin the modernization program.

The as-a-service approach, along with better, faster network connections and security tools are reducing the risk associated with this transformation both from technology and cultural perspectives.

In this e-book, we interviewed five Air Force leaders in the policy, acquisition and operational communities about the current state of the EITaaS risk reduction pilots and their expectations going forward.

The service's IT executives are focused not only on getting the right technology in place, but also relieving some of the burden on managing the network, the user devices and common software requirements.

Maj. Gen. Kevin Kennedy, the assistant deputy CIO for digital transformation at the Air Force, said with information technology being so vital to the service's current and future successes, moving to the as-a-service model may be the only way to keep up with the speed of change.

Maj. Gen. Michael Schmidt, program executive officer for command, control, communications, intelligence and networks, offered insights into why EITaaS is about getting the best from industry and not the same old, same old.

And Brig. Gen. Chad Raduege, the director of cyberspace and information dominance and chief information officer at Air Combat Command looked to the future of the program and how it will help the service finally satisfy airmen's insatiable appetite for IT.

Taken together, these interviews paint a picture of where EITaaS is today and what the Air Force expects from it in the future.

Jason Miller
Executive Editor
Federal News Network

FEATURED AIR FORCE EXECUTIVES:

Maj. Gen. Kevin Kennedy, assistant deputy CIO for digital transformation

Maj. Gen. Michael Schmidt, program executive officer for command, control, communications, intelligence and networks

Col. Bobby King, senior materiel leader, enterprise IT & cyber infrastructure division

Brig. Gen. Chad Raduege, director of cyberspace and information dominance, and chief information officer at Air Combat Command

Col. Brenda Oppel, the director of the functional management office for the EITaaS risk reduction effort

EITaaS Perspectives from the policy community

Jason Miller, Federal News Network executive editor, talked with Maj. Gen. Kevin Kennedy, the assistant deputy CIO for digital transformation at the Air Force. Maj. Gen Kennedy has the lead policy role for EITaaS at the Pentagon.

Miller: What is your role with Enterprise IT-as-a-Service, and what are your focus areas?

Kennedy: My role as the director of digital transformation and the assistant deputy CIO is I provide the Headquarters Air Force-level oversight of the activity, and then ensure that the coordination across the Air Force happens to roll out Enterprise Information Technology-as-a-Service. And in that role, I handle the costing, the forecasting for our budgeting and also the strategy and the vision of where we want to take the initiative. We're closely partnered with Air Combat Command just down the street at Langley Air Force Base, and also with our acquisition professionals up at Hanscom Air Force Base. What I do is look across the portfolios to make sure of how we're going to provide information technology to our airmen, and also the Space Force, to make sure that we're ready to accomplish the mission. I'm also the assistant deputy chief of staff for cyber effects operations. In that role, I'm thinking more about how we're going to leverage the network that we're fielding, leverage information technology and the capabilities and applications it supports in warfighter communications, and then cyber effects operations.

Miller: Enterprise IT-as-a-service is very interesting because this is not one of those things where you guys are saying, 'Okay, let's just move to email in the cloud,' or 'Let's pick up these applications and put them over here.' It's actually an experiment in many ways. Can you talk about how the strategy, the vision, the budgeting kind of deals with the fact that this in many ways is an experiment?

Kennedy: We are in a risk-reduction phase right now, and what we're looking at doing there is understanding how we procure IT with the capabilities and modern 21st century tools that leverage industry's speed of delivery and innovation, leverages innovation we have inside the service, and also takes best advantage of the military and civilian airmen that we have working in the field.

We didn't want to necessarily have industry just come in and do a traditional acquisition where we set very definitive requirements for so many users at so much time with so much capabilities, and then procure a contract that puts folks in seats to do that type of activity. What we wanted was to consume IT as-a-service, so as the industry model changes, we can also pivot as we can consume it and tailor it to the wing that we're supporting.

As we're thinking through that, there's a few things that we needed as we're in this experiment that we're focusing on. The first one is we're looking at the maturity level of what that capability is that we're fielding. [We] want to make sure that the solution that industry can provide is mature enough to meet the rigors and resilience that we need for our force.

The other part is a very big shift [around] the way you approach security on our network. We are looking at how we enable a pivot from boundary defense more toward data-centric defense, and more toward a zero trust approach. That's a heavy engagement with our industry partners and with 16th Air Force and U.S. Cyber Command and the Defense Information Systems Agency to understand, 'How do we do that and move forward?'

The other part of it is, information technology is absolutely vital to our airmen getting their mission done. It's a time consideration, but it's also how do they get access to the information so they can turn aircraft, fly satellites, make sure our airmen are well trained and prepared to fight and win.

And so we need to think through how the actual information technology is performing. The last one is we have to make sure we're getting return on investment for the taxpayer and that the solutions are affordable. The way that we model and cost this has to be laser-focused on getting the most value that we can out of the dollars that we spend and understanding how we can move that spend, whether it's at wing-level or at the corporate Air Force level, or whether the capability we provide is tailored for the airmen for the capabilities they need. But we don't necessarily want one-size-fits-all across the force.

Miller: I want to go back to one thing you just said about affordability and cost model. This concept of as-a-service is not necessarily new. You've seen it over the years as seat management. We've seen it over the years as the contractor-owned, contractor-operated model or the government-owned, contractor operated model. Why is Enterprise IT-as-a-Service different? Why does this model potentially have more likelihood of succeeding?

Kennedy: I think there's a lot of truth in that question. Where the technology has come in, and what the cloud enables us to do, is enable less of a capital investment potentially into information technology services, the number of data centers and things like that, so we can think differently about it. I want to emphasize we're not looking at EITaaS necessarily as a cost savings [initiative]. There's two challenges that the Air Force asked us to look at. One of them was a capability improvement – the speed and resilience of IT that we needed to improve. And the other part was they wanted the most modern kind of capabilities that were out there. Where we are on the model is trying to understand what we need to have built in to the acquisition roles that incentivizes the right behavior. I think a lot of our risk reduction effort is also looking at how we write contracts in a way that doesn't disincentivize the outcomes that we're looking for.

The other part of is that we need to make sure we don't have a vendor lock-in situation as we're going in, make sure that our data is mobile and portable, especially if we need to go a different way.

Miller: Some of the metrics of success that you're seeing seem to be around the vendor lock in and the data mobility, the as-a-service model. What are some of the other metrics you're paying close attention to?

Kennedy: There's the kind of mission readiness metrics that we look at, which is at the core of how our airmen perceive their information technology and is supporting their mission. We see this as a readiness issue. That's one of the things that we're capturing with a pretty robust regime of surveying our airmen as they're out there consuming the services across the Air Force networks and as well as at the risk reduction bases. Another of the things is the lessons learned on the execution side of the house, with respect to the acquisition vehicles that we are going to roll out as we look to go to production in 2022 and 2023.

The security concept of operations development is another metric; the maturity model of how we do incident response, where the lines are between industry and Air Force cyber to make sure that we have the ability to continue to maneuver and, when necessary, take action on our networks, if adversaries are inside trying to access our data or prevent operation of our network.

Miller: Can we look into the mission readiness issue a little more? When you talk about capturing the survey, how do those work? And maybe even just at a high level, what are some of the things you're learning from those airmen?

Kennedy: Absolutely. As you're on working on a network, it's a series of questions that ask about the satisfaction level with a network. A question tree leads you down a path to get a sense of what our airmen think. Then, we look through the free-response answers, where we see how many times things are mentioned, and how many times they are mentioned in a positive or negative manner. Most of the time our airmen like to come out and highlight a lot of the positive things in their comments, but that's also where we find the real pain points, so we can understand where we are in our network. And what we're finding is in the past decades, the way we've constructed the AFNET has been successful in many ways, but it also has

created a problem: a non-efficient transactional path, in some ways, to get different capabilities. We cobbled together different parts of the network to form the AFNET.

That's one of the things that we determined about the network from those responses, and they enabled us to really look at some of the pain points that were enabled, like slow access to email, slow access to information in our Office 365 environment. In the last couple of weeks, we've gone through and simplified that transactional path within the Air Force. For some of our airmen, it was 48 potential steps to get in and back. We were able to bring that down to 20 to 25, depending on how you're accessing the network and what information you were trying to use. That was one of the things that the survey helped us identify.

We continue to look at that transactional space and focus on our airmen and their ability to leverage the network and the end user devices that they were using. We needed to understand if our technology refresh rates were keeping up with the capabilities, and we were also looking to explore the kind of tools that we're using in the cloud. That was one of the other things that we highlighted: as we do our follow-on technology refreshes, what are the baseline capabilities that we want in our tablets or laptops or desktops?

Miller: As you guys have rolled out Enterprise-IT-as-a-Service, there's obviously a lot of things that are happening at once. I think you guys have three or four different proofs of concepts, three at the risk reduction bases, and then you're working with some other agencies, whether it's on the user, desktop management side or even with Google looking at potential move to zero trust. Give me a sense of what some of the broad challenges have been, and how has the coronavirus pandemic added to those challenges or impacted the program?

Kennedy: First of all, some of the broad challenges of moving toward an EITaaS environment is just the cultural change. As for the technology, industry and the Air Force understand where we need to go that will enable us to consume network-as-a-service.

With our two primary partners there being AT&T and Microsoft, the technological solution was understood, though not simple. It says you will enable Air Force information to leave an Air Force base-area network into an AT&T or Microsoft network. We're still in the early stages of doing that up to full capacity, although just on May 29, we were able to approve both Offutt Air Force base and Buckley Air Force Base to go from a 10% capacity on their network-as-a-service up to 100% capacity. That throttle is being guided by the 16th Air Force down at AFCYBER.

The other part is there is a stakeholder engagement piece that we needed to really focus on between industry and the base-level airmen that are working toward this new way of information technology, as well as at the headquarters level and the major command level to make sure that all of the stakeholders across the environment understand what we're trying to do.

The key here is we're looking to provide services at an enterprise level, and cost and resource them there, where previously it may have been the requirement of the major commands to do that. With that there comes some expectation that the resourcing will also move to headquarters, and with that comes the responsibility for the headquarters to make sure that major commands understand what we're doing with those resources and are fully involved in the decision making.

The governance model that we're employing has been an incredibly significant part over the last couple of months now with the coronavirus response. What we found is our industry partners were able to continue moving along on many, if not all, of the lines of effort, even though mobility across the nation was limited. Some of the activities may have taken a little longer, but we think we can make that up in schedule as we move forward. That is something that we're monitoring.

The folks that had already rolled out capabilities – for example, at Buckley Air Force Base – the base-area networking support that AT&T was providing there was able to come into this new environment and help the base think through how they provide virtual private network access in different places

that weren't on the base before, and roll that out. They figured out how to provide extended SIPRNet classified networking into other spaces to help with the dispersing around the base, so we could decrease density or make it possible to work from a remote station.

Additionally, SAIC, who's leading one of our efforts as far as our service desk responses and ITSM functions, also stayed up and running fully through that, and that helped us quite a bit with the Buckley Air Force Base virtual private network responses. What we saw during the pandemic was industry was able to continue to provide services, much like we saw industry providing an incredible amount of telecom support to the nation.

Miller: You mentioned the Offutt and Buckley Air Force Bases are basically going from 10% to about 100% or close that for network-as-a-service. What does that mean?

Kennedy: What we're trying to see there is how we can leverage a different transactional path with different security devices that will enable us to leverage their networks or security. We are looking to see if we're leveraging their networks, their cloud access points versus the ones on the DoDIN transactional paths and see if there's a difference. We want to make sure that we're comfortable with the security on that path as we're transitioning along.

Miller: If we have this conversation in a year from now, or five years from now, what will the network look like? What will it mean to airmen?

Kennedy: In a year from now, our expectation is to be in a place that we have the planning and the strategies in place to roll EITaaS across the force. It won't be the entire Air Force and Space Force – not every member of both services will have that, but we're looking to have our planning and our acquisition strategy well aligned, our manning strategy well aligned, and our cost strategy well aligned a year from now. That sounds like a heavy lift, and it is. But that's where we're looking to be in a year.

As for where we are going five years from now, we look to have what we're going to have for capabilities in the EITaaS model fully up and running. We are still in risk reduction, so we have to understand as we look at our lines of effort – compute and store, network-as-a-service and user services-as-a-service – what capabilities that we do continue in an as-a-service model. I don't want to leave you with the impression that it's going to be all lines of efforts, all fully as-a-service. We still very much have an open mind about how we're going to be able to provide the capabilities, but the bottom line is that our major commands and their leadership have challenged the CIO and the Air Staff to provide a capability that enables mission readiness for the future.

Miller: There's a similar effort going on at the Army. We know that the Navy has been down this path with NMCI and NGEN. The Fourth Estate has been working on very similar consolidation efforts. Walk me through how you are working with those other services and sharing the lessons you've learned and pulling in their lessons learned. How's that communication happening?

Kennedy: There was absolutely partnering, looking across department for lessons learned as we constructed our as-a-service approach to this. One of our first conversations with the Navy was to understand what they felt was well-executed, and what they felt they would change if they had to go back and do it again. We have a new model that wasn't necessarily allowed when the Navy started this. One of the key points was looking at how they rolled out their change management, how they rolled out across their workforce, we took all those lessons on board.

The Army has partnered extremely closely with us and has their own initiative. It is a slightly different approach, but they are working with us to the point where the Army has embedded liaison officers with our integrated program office up at Hanscom. We have provided occasional updates to the DoD CIO. We also get together with DISA just to make sure we're all understanding where we are and to see if there's any friction points that we need to work through, as far as coordinating some of the technological solutions or some of the policies between the Air Force, the DoD CIO and DISA.

One of the things that the Air Force signed up with the DoD CIO is as we look at our security requirements, the commercial solution needs to be equivalent or better, and that's one of the things that we're holding very fast to as we go forward. We also have operational readiness reviews as we roll out key capabilities, and one of the very significant discussions that we have during those reviews is the security posture as we're moving forward. But that's how we're looking to stay synched across the department and be transparent with our key partners: DISA, the DoD CIO, U.S. Cyber Command and the Army.

Miller: When you work with the Army or work with the other services, are they on the floor with you, or do you tend to kind of catch up with each other on progress and challenges and the potholes to avoid at other times?

Kennedy: The primary mechanism is the Army is integrated into our integrated program office. We're also working DISA to have a field office with DISA up at Fort Meade and have a dedicated person that's identified there to be an Air Force representative. The Army already has someone embedded up with us at Hanscom, and we also have the ability to embed DISA as we move forward if that becomes a demand signal as well.

Miller: One last thing comes to mind as you bring up this idea of Enterprise IT-as-a-Service. How's it going to change the role of the airmen, the people who support the network and technology today?

Kennedy: Although our vision for this would be a decreased role as we require our airmen to be more adversary focused in the space, we need to figure out how we can move them more into defensive cyber operations and mission assurance – the primary vehicle for that being our mission defense teams that we're looking to roll out across the Air Force to ensure that we can generate air and space power across the Department of the Air Force. We will still have airmen that will be involved with information technology, but the numbers will decrease. Their focus will become more adversary-focused, and on integration of our warfighting capabilities rather than on pure service delivery.

EITaaS Perspectives from the acquisition community

Jared Serbu, Federal News Network deputy editor, talked to the acquisition leadership team for EITaaS: Maj. Gen. Michael Schmidt, the program executive officer for command, control, communications, intelligence and networks, and Col. Bobby King, the senior materiel leader who is responsible for life cycle management of the AFNET.

Serbu: As an initial matter, talk a little bit about your role in EITaaS. What's the PEO's role, and how do you plug in and integrate with the rest of the broader Air Force and DoD team that has a hand in this big effort?

Schmidt: That's a great question. Because this isn't your typical situation where you get a set of big requirements and then wait 10 years and end up with an airplane or a widget of some sort. This program really requires a great deal of collaboration between the acquisition community, the operational community and the policy community.

But as the Program Executive Officer, I have a pretty broad portfolio of programs across the cyber and crypto side of things, the aerial networking side of things, and in this area, the enterprise IT and cyber infrastructure side of things. I probably have about 300 programs overall in the portfolio, but Enterprise IT-as-a-Service certainly is a unique one. And the effort that we have embarked on right now is our risk reduction effort, really to inform the broader acquisition strategy.

The acquisition strategy is delegated to me for the risk reduction effort. My boss, Dr. [Will] Roper, the Air Force acquisition executive, will be the acquisition executive for the broader EITaaS program that that will be informed, of course, by this effort.

That might not sound that innovative, but I really think it is. We collectively convinced ourselves that we need to have an integrated program office where we have those operators and policy people and acquisition people all sitting together in what we call our integrated program office here at Hanscom Air Force Base.

Additionally, we've had a strong partnership with the Army pretty much right from the beginning, and they even put a couple people on our team here at here at Hanscom. That's definitely unique about this acquisition program, and I think I would love to have it in some of those other big widget programs. But in this case, I think it's absolutely required that we have that kind of an arrangement.

Serbu: The integration piece is interesting. I think it's been about a year since that the functional management office, which I think is owned by Air Combat Command, opened up under the same roof with you there at Hanscom. How has that worked so far? What has it enabled you to do, or to do better?

Schmidt: From my perspective, it allows us to recognize that there's no finger pointing that is even useful in this discussion. We're all doing this thing together. It's not those acquisition guys or those operators or those operators or policy people who don't know what they're doing, because those people are all "us." And so that part of it is really unique.

King: The IPO is headed up by three Air Force colonels, and it's been phenomenal, because Col. Gerald Yap actually sits in the Pentagon, along with a couple of other people that are part of the IPO, helping with the policy pieces. As you can imagine, since this program is so different, the scope of what we're trying to do involves lots and lots of strategic communication going on in the Pentagon. But Gerald and Col. Brenda Oppel *(see separate interview, p. 13)* and I talk at least three times a week – sometimes three times a day – to try to move as fast as we can to deliver these enterprise

IT services. And it is so awesome having a full time O-6 from the lead major command working to help ensure that this program is successful. We work very closely to make sure the policy pieces are well integrated with the acquisition pieces and vice versa, so we can go at a much faster pace than in your traditional process where you wait on the requirements from the lead MAJCOM and then try to deliver a program.

Serbu: I want to talk a bit about where things stand. I know we're still in a risk reduction phase, but that's the same moniker the Air Force has placed on EITaaS for quite a while now. So as a practical matter, where are you on this journey? How close might you be to getting to a place where something called EITaaS is rolled out across the entire Air Force?

Schmidt: I think the speed at which we roll EITaaS out to the whole Air Force will be budget dependent, and the risk reduction effort will drive a discussion that will drive how much the Air Force can afford to invest in this.

Today, we have six risk reduction bases for the network as a service. And then for end user services, we have eight risk reduction bases, and the same with compute and store. So as far as end user services, that's rolled out to all the bases and airmen in the risk reduction effort, except we're still working through Spangdahlem Air Base.

But as part of the end user services, we really want to put a new image on our desktop that optimizes [the user experience]. Just think about the path that your computer has to take when it starts up, including all the all the security things. That image is not yet released, but as far as the helpdesk, trouble tickets, who you talk to to get your problems fixed, that's already rolled out at the risk reduction bases.

There's a constant tension between ensuring cybersecurity and wanting to go faster, and that is definitely something that we've learned during this risk reduction phase. So we started out by rolling out to 10% of the users at Buckley Air Force Base, then 10% of the users at Offutt Air Force Base. We've just recently gone to 100% of the users at Buckley and Offutt, and I would say we were 10 times faster at the second base than at the first base. So that really gives us a lot of confidence that once we do get funded, we'll be able to scale to the Air Force in a significant way. Buckley and Offutt both used the AT&T solution. The next big turn-on is 10% of the users at Maxwell-Gunter Air Force Base, and that's the first Microsoft base.

I would say one thing we've definitely learned – and we kind of knew this – is that if you've seen one base, you've seen one base. And really understanding the architecture at each base is a really important part of this. The companies are out there ahead of the next base getting all that set up, but the work they're doing is honestly a result of years and years of underfunding our IT infrastructure within the Air Force.

We've funded it in a way that we just scrape up whatever money we can find in the execution year, and kind of limp ourselves along from an IT perspective. So taking this holistic look, not only at each base, but then at the whole enterprise is a huge part of this risk reduction effort. Once we've learned how to get through that, it's a much quicker process.

Serbu: Just to pick up on your "if you've seen one base" comment, I wonder how true that will be when you reach whatever the end state is. Is it an objective to make this Air Force network a unified enterprise network that kind of looks the same in every place, or is it heavily tailored for each MAJCOM and for each base's mission requirements?

Schmidt: The wide-area network is definitely something we want to implement across the Air Force and standardize that. How we do help desk and end-user devices and end-user services is definitely something we want to standardize across the bases. We want to take advantage of commercial internet access solutions in a standard way and have a competitive process to continually take advantage of commercial products across the Air Force in a standard way.

When you get to each base and make the initial assessment of what they have and what they don't have, some are more modern than others. Some are better laid out in terms of understanding how

to connect from each of the buildings to, let's say, the central networks, then other bases.

The team is getting really good at quickly identifying what is different about this base than that base. But from my perspective, we are not tailoring a solution for a base. In fact, just the opposite. We have huge bases, we have medium-sized bases, we have small bases, but to the maximum extent possible, we want to not have their differences affect their performance in any way.

Serbu: You mentioned how tightly-linked you are with the folks in the Army who've followed down a similar path. I wanted to ask you what you've learned from the Navy so far. They have had a heavy industry role in managing their IT enterprise for 20 years now, and senior Navy leaders will freely admit that even though that's the case, they think they're about 15 years behind the technology curve. That's obviously not where you want to be. So how clearly do you think you understand, at this point, how to actually contract for IT services a way that incentivizes or requires industry to really deliver the state of the art on a year-by-year basis?

Schmidt: That's a really good question. Our teams have worked really closely with the Navy to understand what they have learned. And the Navy philosophy, from my perspective, is that they went into this thing trying to hire contractors to replace the organic operators and really just bring in services to run their IT enterprise.

We, right from the beginning, did not want to do that because we did not want to just bring people in to manage the same old network and the same old technology, and just have different people running the same unacceptable network for the Air and Space forces.

So right from the beginning, we divided this up into network-as-a-service, end-user services, and compute and store, to specifically go after only the best in the commercial industry in those specific areas. And that's how we went through the [other transaction agreement] (OTA) process to really allow the best in the commercial industry to compete within those areas to give us their best solutions in those areas.

In the long term, when we go into full production, whether we stay in those three separate pockets or not, it allowed us to get to the best commercial providers in those areas and bring their "A" game.

King: In the beginning, before we even got to the point where we decided to use OTAs, we spent a lot of time with the Defense Innovation Unit as well. And they helped us a lot with figuring out the initial strategy for the OTAs that we ended up using. But as far as how we're going to ensure that we keep modern technology in the production contracts, that's not something we can really talk about until we've got the acquisition strategy figured out and it's public knowledge.

Serbu: Not to go too far down a rabbit trail of contracting procedures, but any observations you'd like to share about how that OTA route has worked for this specific effort so far?

Schmidt: In this case, we were really wanting industry to bring their ideas to our problem, versus us telling them what all the specific requirements are and then just going and executing. The OTA process allowed us to give a broad statement to industry saying, "Hey, we want you to bring your best and brightest to attack this problem."

Unlike a regular source selection, it allowed for a very collaborative environment to really understand what the company was proposing to bring or not proposing to bring. To me, that's the best part of the OTA process. It's different than a closed-door source selection.

We made it as competitive as possible. We used the Gartner standards and we invited the best in the industry that were recognized in those areas to submit papers, and we whittled that down to a number of white papers. But having that collaborative discussion before we really got going was really a great part of the OTA process as we went through this startup phase.

Serbu: Can you clearly see from here how you maintain that level of continuous industry engagement and continuous influx of ideas, instead of getting into a vendor lock situation once you get into production? As far as that environment where

you have constant two-way communication with industry, can you see how you maintain that over the long haul, 10 years from now?

Schmidt: I can. Certainly, ownership of our equipment and our data is a big part ensuring that we don't get into vendor lock, and we do have a number of courses of action that will ensure competition into the future.

Serbu: Along similar lines, I'm imagining that at some point, once you do get into production, there's going to be some fairly clearly-defined lines between what airmen do for you on the network and what industry does for you on the network, and likewise, what the Air Force owns versus what industry provides as-a-service. At this point, do you know where those lines will be drawn, or is that still part of the risk reduction exploration?

Schmidt: That's definitely still part of the risk reduction exploration. On the one hand, we would love to repurpose as many of our government personnel as possible to the mission defense teams

on our cyber side, and get them out of the business of having to run the day-to-day operations of our network and our end-user services.

That said, I think there's a cost factor in all of this. This risk reduction effort is going to help us decide how much we can afford to do that, and what that business case looks like. Additionally, when we holistically manage all of our network and our end-user services, we have an opportunity to manage with a networkwide and servicewide security operations center.

We're still trying to figure out how much we can do centrally versus having to do from base-to-base, communications squadron-to-communications squadron, and the risk reduction effort will inform that. But that's going to be key in aligning specifically what airmen will do in the future versus what they do today.

Serbu: Once you actually have production contracts awarded and you tell industry, "Go build the network," what's the long-term government oversight role over that whole process? How do you keep watch over what's actually happening on the ground? Does that fall to the integrated program office, or ACC? Do we know yet?

Schmidt: This is all being fed by the risk reduction effort right now, and it's a really good question, because certainly the security of our networks falls into Air Combat Command, and specifically the 16th Air Force. Certainly the oversight of the security side of our network will remain their responsibility. How that relationship works with the contractors is definitely what's being developed right now.

From an acquisition standpoint, certainly there will remain an oversight of the contractors and their performance and their tracking of the metrics against contract requirements. That will remain with the acquisition community, I would expect. But once we make the full shift to EITaaS, it will be much less burdensome to the Air Force than it is today. Because if you think about it today, there are so many people that have that role, whether it's the formal program offices that I have in a bunch of programs that are just taking care of the legacy networks, or whether it's each base's communication squadrons and their oversight of contractors at their bases, or what the 16th Air Force is doing in their oversight, we are definitely going to be able to streamline that significantly. Again, this risk reduction effort is informing that.

Serbu: I just want to take a quick detour on the money question. You've mentioned a couple times that the pace of the EITaaS rollout is going to be budget-dependent. I just want to make sure it's not the case that you think EITaaS is going to be more expensive to run than the current AFNET structure once you get to a steady state operation. I assume the pacing question is mostly about upfront costs?

Schmidt: No, we do not expect this to be more expensive. We never went about EITaaS to save money, we did it to give our users an opportunity to better meet all of their mission execution requirements, and provide a better user experience to them.

All of our cost estimates have validated to us that we can do that at about the same level of funding that we are spending right now today. The one little "gotcha" in the whole thing is obviously when we're investing in EITaaS early on, our legacy network still must keep running. Our Air Force isn't just going to stop while we make this transition. We do expect there will be dual costs that need to be paid to implement the new while maintaining the old.

Serbu: I want to dig a little bit into the current COVID situation, just because it's changed so much how we all consume IT services. I think we're all still trying to figure out how permanent those changes are. But having observed the way the Air Force and the rest of government had to adapt to that situation, has it changed at all the way you think about how EITaaS needs to be architected?

Schmidt: It definitely has changed things. Before, at least we knew how much we needed to really change our air and space folks' user experience, and we've now added the telecommuting side to all of this. COVID-19 has actually been a great thing for our IT business in general: conversations at all levels, relative to funding to some degree, but

also security conversations that really needed to happen are really starting to happen.

I'm really proud of Col. King's whole team and Air Combat Command and [the Air Force CIO's office] for delivering what they've delivered, improving access from off base by about 20-fold, with a lot of new tools that continue to comply with security requirements, and there are all kinds of really innovative discussions about those tools.

COVID took some of the same people who've been working on EITaaS and made them think about all these telecommuting things in the short term, but it also got conversations going, whether it's in the Air Force or at DISA or Cyber Command. The relationships we built in 12 weeks way overshadow what we've built in the last two years, just because we now talk to each other every single day, and I think that's going to help EITaaS a lot as we move forward.

I also think the fact that we're not traveling so much, especially on these programs, has really been a benefit. The fact that we're not spending a lot of time on airplanes has really allowed us to focus on this. So overall, COVID-19 has driven our attention to some areas.

At the same time, I think it's freed us up to have more meetings, and to get more attention on the fact that this is absolutely a showstopper if we don't completely change our IT experience in the Air Force. It's focused us on what we need to be able to do to connect from our houses or off-base.

Serbu: To that point, once you are in an environment where the network really is mostly made up of commercial things that are delivered as-a-service, I wonder if it makes it easier to deal with something like this. Because instead of having to go through these herculean efforts to completely change how you're delivering services, you're really just turning up the rheostat on how much commercial network bandwidth you need, for example.

Schmidt: I think that there's some truth to that. It's not quite that straightforward, because we definitely want to connect people through the secure environment, but you're right. And the more we optimize the transactional paths to focus only on the security and to give us the best user experience we can within the security construct, what you're saying would be correct.

Serbu: As you continue this learning process during the risk reduction phase, how much of that feedback is coming from end users? How valuable has that been?

Schmidt: We poll our end users all of the time. They are very demanding customers, as you can imagine. So that feedback is constant and good. And it's not just feedback from the end users, but it's feedback from the communications squadrons, and from all levels within the command. This is something that our leadership in the Air Force and the Space Force – they demand that we get this done, and we get this done as soon as possible. So there is no lack of feedback in this whole thing, I can tell you that.

King: From the very beginning this program, we realized that unless we can show hard data, both on the objective side with network measures and other net performance scoring, as well as the subjective side in user experience, we'd have a tough time selling it, because it was such a big change. So we worked very closely with our chief experience officer in the Air Force CIO's office in the Pentagon.

We also did face to face interviews at all of these bases that are in the risk reduction experiment from the very beginning. We put in place tooling by AT&T and the other vendors – Microsoft, Accenture and SAIC – to measure the objective performance at the bases prior to shifting users over to the new networks or the new services being provided by the vendors. So we have that good baseline.

And we've also done pulse surveys throughout the Air Force, and we're able to compare the non-risk reduction bases with the risk reduction bases. So there's been a tremendous amount of focus on the metrics so that we can ensure that we find the right areas to focus on to increase that end user experience, while at the same time not sacrificing security.

EITaaS perspectives from the operational community

Scott Maucione, Federal News Network DoD reporter, talked with Brig. Gen. Chad Raduege, the director of cyberspace and information dominance, and chief information officer at Air Combat Command, and Col. Brenda Oppel, the director of the functional management office for the EITaaS risk reduction effort.

Maucione: Discuss your role and how the enterprise IT-as-a-service initiative impacts your focus areas.

Raduege: For Air Combat Command, this story really begins about two years ago in summer of 2018. ACC was appointed as the lead major command for both cyber and enterprise information technology.

In my role as the ACC/A6, we really coordinate on a daily basis with the [Air Force chief information officer] at the Pentagon, our [acting] deputy chief information officer [Arthur] Hatcher, and we also have a role as lead command to build some unity of effort across the Air Force.

Much of my time is spent coordinating with the policymakers, but also building some unity across all of the other major commands and trying to unite on what we're doing. Today's focus is really going to be on that enterprise IT portfolio and some of the things that are going on there.

EIT is your classified and unclassified email. It's your virtual private networks that allow you to be a mobile workforce and most recently during the COVID response. It's all of the collaboration tools. It's your Teams, it's your SharePoint, it's your cloud technologies. It's your long-haul circuits that connect all of the bases together and build out the Air Force network itself. It's all of the mobile users on all the mobile devices that we have out there and how they interact with one another.

All of those are things that fall in the IT portfolio. One of the things that we're most excited about, one of our biggest initiatives, is one that directly supports [ACC Commander] Gen. [James] Holmes, to get to the future faster. That's where this EITaaS comes in. This is a unique environment that we're jumping to, when we say 'as-a-service' that means that we're relying on someone else to provide that capability.

This has been about a two-year effort for us to do things differently. As ACC became the lead command, we established something called the FMO, the functional management office, and this was really to marry some of our ACC lead command personnel with representing the kind of operational Air Force.

As lead command, we represent what the warfighter needs from a key perspective. We took that into Hanscom Air Force Base, established the FMO to work side-by-side with our acquisition professionals. Our acquisition professionals are the ones that actually buy the services that we need. Marrying that requirement to those that are actually acquiring it is exactly what the FMO was designed to do. Not many people liked the term, but I think it is a very good description of what we've asked that FMO to do.

That's created a healthy tension between our needs on the warfighter front and those that are spending the dollars and putting things on contract. It's to find that healthy tension to make sure that they are buying what we need and is most relevant for the Air Force.

Maucione: Col. Oppel?

Oppel: As the general just mentioned, he created that functional management office. That FMO aspect sits at Hanscom Air Force Base. He was able to break away a billet from his organizational structure to create an O-6 billet,

which is the billet that I sit in up here at Hanscom Air Force Base. I represent FMO assets for Air Combat Command. Within the FMO and program management office or PMO relationship, we have built a 106-member integrated program office for this EITaaS risk reduction effort. As a team, we oversee that $400 million, three-year risk reduction effort budget.

What we do is we work together to make sure that the commercial industry services that are provided do meet the operational requirements of our air and space forces. In the FMO aspect, I'm working hand-in-hand with the local communications and cyber squadrons, as well as their group and wing leadership, at those risk reduction effort bases to ensure that we have success and mission operations with no failures.

Further, I feel like I'm the government relations manager to those five Fortune 500 companies that we're working with within the risk reduction effort to solidify the cross-sector partnerships. I also represent Air Combat Command with enterprise IT to the governance group board and council, which we have up at the Pentagon on a quarterly or biannual basis. These are the key decision makers that decide on the priorities and resourcing for enterprise IT. I make sure that we're working with them closely.

Finally, I act as a liaison to some of our other partners and stakeholders throughout this effort. I liaise with the Office of the Secretary of Defense chief information officer, as well as Defense Information Systems Agency (DISA), U.S. Cyber Command, Air Force Cyber, Army Cyber, regarding these enterprise IT programs and policies, as well as the different pilot efforts, such as the Army's EITaaS program, which is very similar to ours.

Maucione: ACC has a lot of responsibilities when it comes to combat and staying on the forefront on the operating edge of things. How does EITaaS help you do your mission?

Raduege: Much to my chagrin, but true, nonetheless, is that IT has become a retention issue for our airmen. What we've noticed is that after years of inconsistent funding, it has led to really an underinvestment in our IT infrastructure. It's impacting exactly what we see every day. IT really underpins every single mission in the Air Force – whether it's bombs on target or whether it's spending dollars or managing our human resources – everything is based on an IT infrastructure and IT assets.

We also understand that as we start looking forward to the future, you hear the Chief of Staff of the Air Force talk about the Air Force's role in joint all domain command and control. When he starts describing that, he talks about the highway that allows all of the connectivity between our bases and our forward edge in the battlefield – whether that is an F-35 or an airman at the tactical edge – that information highway is really what EITaaS is all about.

What we've noted for many, many years, especially in the Air Force is that our airmen really have an insatiable appetite for IT. They want to go faster, they want to be more mobile, they want to have cutting edge technology and they want it all integrated with what they experience on a daily basis. That's what's driving us toward EITaaS. A couple of the key benefits about EITaaS is we really think that this is going to allow us to adopt new technology faster. So when you start listening to what's going on in corporate America and they talk about 5G, quantum, zero trust and artificial intelligence and machine learning, those are things that are outside of the of the military that they're doing extremely well. If we can establish a relationship in an as-a-service model where we can get advantages and take advantage of that integration of that new technology, then we think that's going to get us to the future faster.

I think about our commercial partners and what they bring on a daily basis as far as industry best practices. When I go home at night and I'm interfacing with my home email, it is a much smoother process. The processes that are in place, the people and the technology that backstop, all of that delivery is remarkable. It's fast, it's integrated, it's smooth, it's interoperable across the whole globe. That's what we're trying to get at.

I will conclude with this, as far as why this is important for our Air Force. As we start looking at the National Defense Strategy, as we start understanding what the future fight may look like against near peer adversaries, we have to make sure that the airmen that we bring into our United States Air Force are not just providing commodity IT. We have government partners; we have commercial vendors that can do that at scale at efficient costs.

Where we want our airmen to be focused is on the things that require them to wear a uniform and do things like offensive and defensive cyber operations, and then also go forward and extend those networks in the lands of hostility. [That may] mean taking out expeditionary communications or extending a network out or providing connectivity for an F-35 at the tactical edge, or providing the backbone of our command and control across the Air Force.

Maucione: What you do at ACC requires a lot of classified information because you're dealing with combat and forces that are moving. How do you marry speed while also dealing with classified information and are there other challenges you're seeing as you move toward EITaaS?

Raduege: As we move toward the EITaaS environment, as with any big change, change is hard. We're seeing that right now. Part of that change is in our IT workforce that we already have in place. So this is not only the IT, but the cyber workforce, and how those two forces interact. One is primarily concerned with the security aspect, and the other one is trying to lay in capacity and availability of data. It's a critical balance that you have to find. So one of the challenges that we're working through right now is how do you find the sweet spot of security and availability.

Change is also hard for our customers. They have joined the Air Force, they have been accustomed to what we provide on an unclassified and classified computer system; things are going to change. Our end users are going to have to adjust as well and we understand that.

I would also highlight that anytime you go through a massive change like we're going through, this is not like you just go in and turn in the old car and get the new one and drive off the lot. I describe it as you have to paddle with two canoes – you have a foot in each – you have one with the legacy infrastructure that is in place and you have one with this exciting new infrastructure, new processes and new interactions. But, you have to paddle both for a time period until you can eventually get rid of that one legacy canoe and jump completely to the new environment. Those are some of the challenges and some of the burning things that we're seeing right now.

Maucione: How do you say 'I think we're doing alright with this canoe?' How are you measuring that and how are you measuring the feedback from your airmen as well?

Raduege: What we have done from the very beginning is we have put in a robust risk reduction effort. This is the initial tranche that our Air Force, and our program office, led by Col. Oppel is evaluating. Part of that risk reduction effort was to evaluate a whole bunch of diversity upfront to try and see from the Air Force perspective. Is it going to give us the gains that we're looking for? Is it going to account for all of the missions? So as you look across our Air Force of where we're trying this risk reduction effort and evaluating right now, you will see a lot of diversity – multiple vendors, unique solutions, different bases that have different populations, some are very civilian oriented, some are mobile, some are big, some are small, some are primarily focused on education, some are flying operations from their base on a daily basis.

We have also taken an approach where we need to measure the user experience, we need to understand some qualitative and quantitative user feedback before and after, so that we can gauge whether this is really delivering what we want.

Oppel: From a qualitative perspective, we're reaching out to the users through our chief experience officer, Mr. Colt Whittal. [He] is working with the Air Force survey office to send what he calls a pulse survey. That pulse survey does hit

about 1% of the Air Force's population every day to include our risk reduction effort bases. Through the dashboard, we're able to parse out the evaluations of the risk reduction effort customers to say how they feel their user experiences at their installation with the EITaaS instance there. It looks like those user experiences are positive and trending upward, which is great to hear.

Additionally, each of our vendor partners has quantitative tools that they bring with them with our commercial solutions to measure the bits and bytes. In other words, we have been able to quantitatively show that the AT&T network path traverses for the user 4.6 times faster than the AFNet. Obviously, that would equate to some user experience performance increase.

Additionally, we're making sure that we capture all of the lessons learned as we go through the different risk reduction efforts. Those are the types of things that we need to assess before we are able to go into EITaaS production.

Furthermore, we are engaging with 16th Air Force to make sure that our commercial solution is secure. We're using a subset of their tools as well to make sure that we know that the commercial vendor partners' network is good for us.

Maucione: Once you get off that legacy system and continue forward into your future network, what does that look like? What's your ideal, moonshot EITaaS solution?

Raduege: What we see in the future is an infrastructure and Air Force network that is equipped with commercial standards, the most robust infrastructure that you can imagine. It's one that's mobile and fast and is able to keep up. One that is able to integrate in the new technologies, like 5G, artificial intelligence and machine learning. One that can adapt to the user needs. One that can be predictive in the way that it looks at the data that is coming in and makes decisions accordingly. One that's going to be based on a very high user experience, where we will have feedback that immediately goes in to the system, and we're able to adjust as appropriate. As emerging requirements come in, [the future network] can automatically understand those emerging requirements, and deliver the technology associated with delivering upon that. We see a very bright future and we base that on what we see outside of the Air Force network that we would operate on today. It's what we see when we go home and we're on a commercial network from the house. That's what we envision in the future.

Maucione: How are you sharing what you've learned with the other services? Are you doing that? And what are you hearing from them as well?

Raduege: Yeah, absolutely. I will tell you that as we went into this EITaaS effort, we looked at some history. The Navy had a lot of history with their [Navy-Marine Corps Intranet]. We looked at that approach to make sure that we didn't repeat any lessons that they learned on that. Some of that means who do you put in the seat versus going to an as-a-service model. How do you make sure that you built in competition? How do you get the right people on the advisory committee to make sure that you understood those lessons? So from the Navy, we learned a great deal by studying what they had already done years ago and evolved our way of thinking based on that.

With the Army, I will tell you that we were really the first mover on this on this Enterprise IT as-a-service approach, but we found early on that it was important to bring along someone else; and the Army has been a great partner with us. Part of that is engaging at the policymaker level. Col. Oppel talked about the interactions that are required at DoD CIO and at DISA and how we interact with Cyber Command to really push the envelope a little further and faster. We have also partnered at the tactical level with the Army by embedding some of their folks with the Col. Oppel's team.

Oppel: We have a lieutenant colonel Army officer from ARCYBER who's physically sitting with us at Hanscom facility for the Air Force EITaaS program. We pass back and forth through that liaison officer all the lessons learned that we're experiencing. I would say that the Army's risk reduction effort for their EITaaS program is about six to eight months behind us. They have

had leaps and bounds in their schedule just because of the lessons learned that we provided to them.

Additionally, the Army also is working with a PMO/FMO construct and I'm in weekly communication with those O-6 leaders in the Army as well to make sure that we're not repeating the same mistakes that our program here in the Air Force has. [They were] minor mistakes, but obviously we don't want to slow anything down, so the Army is going to be learning from that.

Maucione: Everyone is being impacted by the coronavirus right now, how's the EITaaS program holding up and are there any changes in operations you've seen from it?

Raduege: I have been very pleased with the way our risk reduction bases have responded. What we've noticed is that a typical Air Force base before coronavirus is working 24/7 to provide installation services, IT to the workforce. Post-COVID they've had to do the same thing. As we have gone through the COVID response,

what we have seen is that AT&T and SAIC at bases like Buckley and Offutt have been able to maintain that 24/7 service, both on site and enabling the remote technicians. They have dealt with the health conditions set by each base. They have dealt with the COVID restrictions that have been placed.

There have been some specific things that I would just highlight for you. SAIC at Buckley has responded to 300 virtual private network users that needed access. SAIC at Maxwell dealing with walk-ins who are trying to get mobile environments set up and virtual private network connectivity. At Joint Base Elmendorf-Richardson, they actually stood up a crisis action group to help deal with the COVID response. And lo and behold, AT&T was there as the infrastructure provider to enable that stand up. We have seen fantastic support, what you would accustom from any airman in a COVID response. We have seen the exact same support from our government partners and commercial partners as well.

A little leeway goes a long way in Air Force EITaaS commercial delivery

THIS CONTENT HAS BEEN PROVIDED BY AT&T

When the Air Force was tackling how to implement IT services throughout its multi-faceted organization, they reached out for help. Six years ago, they asked industry partners, including AT&T, how they could do it better. That kicked off a journey that led to innovation, creativity and eventually a pivot to a transformed and modern IT service delivery.

This journey began with an effort to understand the intentions and objectives for these services. What kinds of constraints, real or perceived, might be out there? What were the policy issues that need to be addressed? Were there technical challenges in establishing requirements to deliver these services and capabilities to the Air Force?

The first priority was to address the seams that result from attempting to interconnect hundreds of disparate networking systems.

"Seams disrupt and impact the ability for uniform delivery of services. If you think about it from a data perspective, it's hard for data to work across seams," said Lance Spencer, the client executive vice president for Air Force and Space Force. "The Air Force wants to undertake a digital transformation and achieve data superiority in their various operating environments, but seams sometimes prevent that. We often find that some systems have been constructed over many years with several stakeholders bringing it together. The Air Force depends on an array of solutions that are implemented in different ways. This causes seams and collisions within the architectures that impact performance, security and availability."

Those fractures in the architecture and delivery model, along with the ineffective handshakes and handoffs, enable bad actors to penetrate a system. That's why it was important to start with a uniform model of delivery for optimized service availability.

One challenge was at the policy level. The Defense Department historically built, owned and operated its own networks and delivered its own IT enterprise. That means some very specific policies arose around those practices that were sometimes empowering, but sometimes constraining. At times, it conflicted with introducing commercial service delivery and innovation.

"Learning and collaboration were necessary. We've been able to demonstrate that our commercial security policy meets or exceeds the intentions of the DoD policy," Spencer said. "When we collaborate, the Air Force is handling risk assessments and signing off on our model, as we've been able to deliver the capabilities they require. So their intention has been to use commercial solutions and innovation as much as possible. That has allowed us to continue our commercial delivery with a minimal amount of modifications."

There's often a misconception that commercial solutions are the same as those for consumer, which can make federal agencies – especially the DoD with its high requirements and standards – reluctant to embrace. But these are the same commercial services that very large and complex private sector organizations implement and scale.

It was significant that the Air Force's intention was to embrace industry best practices, including commercial terms and conditions and commercial pricing that leverages investment and innovation to scale at cost.

"The Air Force acknowledges that commercial providers can deliver the kind of service that they need. We've been able to optimize the way we deliver IT services to them. I think it's hugely transformational on how they typically manage procurement. I think it's going to provide them considerable value, performance and improved customer experience in the future as they scale," Spencer said.

And this kind of approach is spreading outward from the Air Force. Spencer said the Army is using an Other Transaction Authority (OTA) to do a risk reduction effort through enterprise-IT-as-a-service. The Army started shortly after the Air Force began its own initiative. The two branches have been collaborating closely on how they move forward and learn from the experience. It's possible that this model could be easily adopted throughout the federal government.

"A commercial model that delivers upon the DoD expectations could serve as a roadmap for other federal agencies who are considering various approaches to IT modernization," Spencer said. "We're supporting the DoD as they transform. And we're making measurable progress toward enterprise capabilities that can serve as a best practice for other agencies."