AFCEA TechNet Air 2016

The Honorable Deborah Lee James
Secretary of the Air Force
Tuesday, 22 March, 2016

Good morning ladies and gentlemen, distinguished guests, Airmen, industry partners…it's an honor to be here. I should note we're in the Henry B. Gonzalez Convention Center, named after Congressman Henry Gonzalez who served in the U.S. House of Representatives for 37 years, and is remembered as being the longest-serving Hispanic Member of Congress. He was by the way a great Congressman, I remember and was in Congress as a member of the professional staff, on the House Armed Services Committee while Henry B. Gonzalez was serving. He was a great friend of my then boss and mentor Chairman Les Aspinof the House Armed Services Committee who went on to become the Secretary of Defense, So this building has certain memories for me because it brings back the legacy and memory of Henry B. Gonzalez.

A special thanks also to General Shea and AFCEA for hosting what is an inaugural event, and I hope inaugural means the first of many not the first and last because I think this is an important event. It couldn't have come at a better time. It was just last week when I testified in front of my old committee, the House Armed Services Committee and I told them, just as I told the other three committees over 6 weeks as General Welsh and I have been presenting the budget that the Air Force has never been busier on such a sustained and a global basis.

As we sit here today, ladies and gentlemen, your and my United States Air Force is working very hard as example to degrade and ultimately destroy Daesh in the Middle East as part of a whole-of-government and as part of a coalition approach.

In the past year, our coalition forces upped the ante against Daesh, flying more than 55,000 sorties in support of Operation INHERENT RESOLVE. And this by the way represents a three-fold increase over the number of sorties flown in 2014. Make no mistake about this – this is a joint fight; it is a coalition fight, but our United States Air Force has shouldered the lion's share of this effort.

Moreover, we have a resurgent Russia that continues to foment problems in the Ukraine, recently announced its intent to modernize nuclear forces of course they complicated the picture in Syria, they are withdrawing except for when they're not withdrawing. So you have got to keep your eye on that ball called Russia at all time.

In addition, we observed North Korea conduct an illegal nuclear test, and a rocket launch within the last month.

And if all this is not enough, we continue to see worrisome Chinese activity in the South China Sea, and certainly there are very important and growing threats in both space and cyberspace.

So I would submit to all of you her this morning there is basically two bottom lines here. The first is that our Air Force plays a key role in each of these areas. We are fully engaged in every region of the world, in every mission area, and we are engaged across the full spectrum of military operations.

Bottom line number two is every single one of the Air Force's core missions depends on information dominance—whether we are talking about delivering Intelligence, Surveillance, and Reconnaissance, or Global Strike or anything in between—Airmen at every level need timely and accurate information to make key decisions and remain operationally agile in all domains. And by all domains I'm talking about air, space, and cyberspace…those are our domains for the United States Air Force.

Our military's technological superiority is being challenged in ways that we've never experienced before, and we can't take these developments for granted. Because if we do, that could put American lives at risk in the not-too-distant future.

Now with all this in mind, my very first trip in the year 2016 was right here to San Antonio. Specifically, I visited 24th and 25th Air Force, which as you well know this is the core of our cyber and ISR force. It's certainly always a pleasure as I get out of Washington and get to visit with our amazing Airmen regardless of their specialties and certainly being here in San Antonio was no exception. And by the way I think my priority was right on to make this my number one visit of 2016.

Now why were cyber and ISR and I'll broaden it, I'll say why was innovation more broadly at the top of my list for 2016? Well because cyberspace is increasingly becoming a contested domain and it's critical that we make ongoing investments today as well as for the future to ensure mission success. And the number one thing combatant commanders always say they want more of from the United States Air Force is ISR, ISR, ISR. So San Antonio had both of those items right here together.

Now also during this same trip after I left San Antonio I also paid a visit to our Defense Innovation Unit Experimental team in the Silicon Valley otherwise known as DIUx and this team is about six months old now.

DIUx is designed to be, I'll call it an innovation hub for us. While it's true this is a Pentagon outpost, it is not like its five-sided older brother. Instead, DIUx identifies emerging and breakthrough technologies created by the high-tech companies and startups in Silicon Valley, while building direct relationships with the Department. Basically, this team on the ground out there is going to help communicate our most challenging national security problems to the innovators and entrepreneurs out there who don't normally do business with us. They'll serve as matchmakers between ideas and opportunities, and help those companies who are willing to give us a try to navigate through the DoD system.

DIUx will be a visible and accessible "point of presence" for the DoD, made up of active duty, civilian, and key reserve component personnel, and once again this is all happening in the Silicon Valley.

After spending time with DIUx, my journey continued and I visited various companies out there to include Google, FireEye, In Q Tel, Facebook, Boot Up World, and Cisco.

Now given that cyber and ISR and innovation more broadly were the themes of this particular visit, everywhere I went I asked certain questions: What do you think is going right in the world of cyberspace and ISR? What's going wrong? What do we need to do more of? What do we need to do less of? How can we work better with innovation

hubs across the U.S. to bring new ideas and innovations to the Air Force? And very importantly, how can we speed this up?

So today what I'd like to do is share some of my thoughts on the cyberspace and ISR challenges that we are facing in the Air Force. And then lay out some of the efforts that we have underway to address these challenges, to include investments in people, technologies, and partnerships.

So let me start with Cyber and here I would like to offer 4 observations.

My first observation having now been on the job a little more than two years is that we need to shift resources from enterprise systems to warfighting systems. SO what do I mean by that? Well here by way of background let me report: The Air Force spends roughly $4 billion on the world of cyber. But the vast majority of those funds go toward operating the network—that is to say keeping things running and fixing things when they break down.

Regrettably, the bulk of our budget is not spent on defending the network, or assuring core missions from cyberattacks, or on developing the types of offensive strategies that we are going to need increasingly in the future.

The same holds true, by the way, for our people. Of the roughly 67,000 Airmen working in and through the cyber domain, the overwhelming majority of cyberspace, intelligence, and acquisition work force professionals are focused on operating the network. A much smaller number, roughly 2,400 highly trained operators, are focused on defense and on emerging offense within Air Force's Cyberspace and the Cyber Mission Force.

So the challenge as I see it is how do we shift over time, both people and money, to get more focus on defense and offense? We can't entirely ever let go of network operations, obviously, because our mission depend on it, but somehow, we have to do better, and I am convinced that leveraging the private sector is the key.

So what are we doing about all of this? Well to begin with we've tried to put more

resources where our mouth is. We've allocated $672 million in FY17 to advance both defensive and offensive initiatives. Offensive capability allows us to achieve significant military effects without putting Airmen's lives at risk, while limiting the cost, the size, and the footprint of our force package.

Our budget fully funds a total force solution of 39 defensive and offensive Cyber Mission Forces Teams to help maintain cyberspace superiority. And 26 of those teams, by the way, are at initial operating capability or greater, and we intend to reach full operational capability for all 39 teams in the first quarter of FY19.

I think this is a good start and we certainly are going to continue this focus. Later today, you will also hear about "Task Force Cyber Secure", which is an Air Force led effort from last year, and led by our Chief Information Officer, Lieutenant General Bender and right after I present Lt Gen Harris from Air Combat Command will present on mission assurance for weapons systems. Quite honestly, we need both.

Both of these efforts are examining cybersecurity across the Air Force, and they are all asking essentially the same questions: what are our vulnerabilities? where do we need to focus our efforts going forward?

In addition, we'll be rolling out a game-changing capability next month that will provide real-time identification and eradication of malware. We've also initiated pathfinder projects to secure avionics software and maintenance systems vital to aircraft operations. So there is a lot going on in this area; stay tuned because they're will be more information forthcoming in months ahead.

My second observation is that the Air Force has probably not been doing an adequate job of training our cyber warriors in strategic thinking, and we need to kick that up a notch.

Like I said before, we devote most of our talent and money today to operating the network. Tomorrow, the emphasis needs to be on functioning and fighting as cyber warriors, defending our networks and core missions from constant attacks, and preparing to go on the offense when it makes sense to do so.

Now to be fair, we are working on all these areas today. But my point here is we have not been investing in training and sufficient critical thinking in the cyber arena, at least not in my judgement. So to this end and in order to do better going forward our Air University at Maxwell Air Force Base stood up a Cyber College, where our Airmen are now learning from leading cyberspace strategists. The Cyber College leverages cyber technology to meet national security strategies in the next decade. The benefit of this college is Active-duty and Reserve forces, sister services and international partners can now study together and innovate solutions to cyberspace challenges that face our Nation.

Two weeks ago, two teams from our Air Command and Staff college students at the Air University took top honors at the Atlantic Council's "Cyber 9/12" Student Challenge in Washington, D.C. This challenge is an annual cyber policy competition for students across the Nation to compete in developing national security policy recommendations tackling a fictional cyber catastrophe. The Air University teams competed against civilian and military teams from across the country, to include teams from Brown University, Harvard, the Naval Academy, Columbia and NDU [National Defense University].

So thanks to our "Fightin' Electrons" and our "Cyber Jedi", they took top honors – those two teams.

Finally this year, we are establishing the Air Force Cyberspace Innovation Center, located at our Air Force Academy, to help our cadets develop similar strategic thinking skills. This Innovation Center will provide a centralized environment where our Airmen can work hand-in-hand with industry, academia, and agency partners to push the leading edge of technology. This rising generation of officers who will now benefit from this effort will have the opportunity to experiment and shape the future of cyberspace operations.

So we're working the strategic thinking angle, and all of this, of course, is in addition to the excellent training already available to our Airmen in our cyberspace career fields and throughout the Air Force.

Observation number three: we need to recruit at all levels, and think about creative new approaches to attract people to our team, especially a certain category of high end programmers and thinkers. Now at 24th and 25th back when I visited earlier this year, I learned that we are doing really an excellent job attracting the right young people and training them in our force. But as people become experts and really senior in the cyber world, private industry can draw them away, and there is no bonus in the world that we could offer that would keep them, if money is the key thing.

Now with us, of course, money is not necessarily the key thing; we have unique offerings. Primarily, we offer interesting and challenging problems, problems that if solved will have a huge impact, and problems which offer young Americans an opportunity to serve their country.

Now last year, the Secretary of Defense announced an initiative called the "Force of the Future", and is rolling out these initiatives under the umbrella of force of the future, over time. The basic principle of the Force of the Future is that we, the military, have to be more open to different ways of bringing in people and retaining them. We need to think about how to retain the experts that we have as well as how to tap into the senior programmers and talent out there who may want to work on what is to them a very cool, short-term project in the Air Force, and what could be to us a project that's crucial to national security.

So how do we bridge that gap? Well I don't have the answers, but let me just offer a few ideas. Last November, DoD launched what's called the Defense Digital Service or DDS. It operates as a "franchise" of the U.S. Digital Service and has access to their resources and their recruiting pipeline. Now the way it works is this: individuals from leading private sector tech companies will take a leave of absence and they'll come to work for us in the Department of Defense on a temporary basis for some finite period of time. So let's say we have three-to-five technical experts who will come on a six-month basis to address the specific, troubling problem in and around software development and software delivery in the Department of Defense. So, we in the Air

Force are watching that model and we are now looking at this seeing how we can leverage such a resource.

Earlier this month, Secretary Carter, launched what he called the “Hack the Pentagon” initiative that is going to be led by DDS. We are inviting vetted hackers to test the department’s cybersecurity under a unique pilot program. So, obviously we are going to be testing and finding vulnerabilities in our applications and websites and networks hopefully before someone else might find them. I’m pretty sure that the “Hack the Pentagon” is the first of its kind in the federal government, and think of it as a cyber bug bounty program. Many corporations like Microsoft, Facebook, and GM now use “Bug Bounties” as an effective means to crowdsource security solutions at a fraction of the cost and time that it takes to develop equivalent solutions in-house. So we’re taking a page out of the corporate structure and the tech companies’ playbooks on this one.

In addition, we are focused on targeted recruiting and hiring of talent in cyber and other technical career fields in a faster way. For example, we established a cell of dedicated recruiters to specifically assist in hiring specialized occupations, including cyber, and as well as some of the STEM and acquisition fields. These recruiters are now able to use Expedited Hiring Authority and Direct Hiring Authority to bring in technical talent much more quickly, which would then avoid much of the traditional and onerous hiring process. Since October 2014, we have been able to use these authorities to bring in a little bit more than 1,600 new employees and we are looking to do more of this in the future.

My fourth and final observation on cyber is that because the world of cyber changes so quickly, we have got to speed up our acquisition processes. In a cyber world where companies like Apple can quickly bring forward new capabilities, like the iPhone, and then iterate to make improvements nearly on a continually basis, and here we are still building five year plans for acquiring capabilities…that is simply not good enough!

We have an industrial era acquisition processes on the one hand who are trying to compete in an agile, digital world. We can’t afford to acquire all capabilities at the

same speed, because we end up giving our Airmen yesterday's technology delivered three years from now. And once again I say we have to do better.

For this reason, we are engaged in efforts to find alternative ways to get technology to the hands of our Airmen faster. And by the way we do have pockets in the Air Force and in DoD overall where we can do things more quickly.

For example there is one great example right here in San Antonio, at JBSA-Lackland, we have a team of Airmen at the Cryptologic and Cyber Systems Division who are rapidly acquiring both offensive and defensive cyber systems in support of 24th Air Force and the Cyber Mission Force utilizing their Cyber Solutions Cells. So this is a great example of pocket but we need to expand upon those pockets and we need to become more pervasive in this approach. We need to do better across the board.

And so that's in part why we started an initiative we call "Bending the Cost Curve", which is a series of initiatives designed to be complimentary to the overall DOD program known as "Better Buying Power". The goal of Bending the Cost Curve is to cut costs, deliver innovation, and/or cut the amount of time required to acquire a new system. We have several areas targeted specifically at reducing our time to award contracts, adopting more commercial-like business practices, and expanding competition among both traditional defense companies as well as those who are not currently doing business with the DoD.

A few weeks ago, we unveiled a new acquisition vehicle—we call it "Open Systems Architecture"…or "OSA". It is using a special authority provided by Congress, called "other transaction authority," that allows us to create novel business structures that wouldn't otherwise be possible under the standard regulations. OSA is specifically designed to accelerate the acquisition process rather than lengthy, lengthy periods of time. We are hoping that this new OSA vehicle will give us an average of about four weeks from proposal receipt to award. Now I am not suggesting that we could use such a vehicle to build a next generation aircraft, but I do believe for smaller types of

technology assertions and enterprise cyber capabilities this is the type of direction where we need to move.

We did successfully demonstrated the OSA concept with our Distributed Common Ground Station (DCGS) program last year. And building on that success, the Air Force Research Lab created a permanent OSA vehicle as I said. It was just rolled out a few weeks ago. We're expecting a much broader group of programs to use the vehicle in FY16 and the future. In order to participate in these opportunities, all companies have to do is to join our "Other Transaction" Consortium. Which is easy; it's a one-page thing. You can go online and fill out and I would encourage anyone here today who is interested to check out at www.transform.af.mil.

Alright let me shift briefly if I may to Intelligence, Surveillance, and Reconnaissance…what we call "ISR". Needless to say ISR is an extremely important mission for the Air Force; it is one of our top five. ISR provides actionable intelligence from multiple sources—including platforms, sensors, people, and databases—and the idea is to provide this information to national decision makers and tactical level personnel. As I mentioned earlier, this is the number one capability combatant commanders say repeatedly that they want more of from the United States Air Force.

Platforms and sensors collect the data and our systems convert the data into information…but it is our ISR Airmen who turn that information into timely intelligence for decision makers: and I'm talking about decision makers from those on the battlefield all the way up to the President of the United States.

The 25th Air Force brings to bear the full capabilities of ISR Airmen and with the inclusion of the 9th Reconnaissance Wing, the 55th Wing, and the 363rd ISR Wing, the 25th Air Force missions expanded to now include electronic warfare, targeting, airborne national command and control, reconnaissance in support of nuclear operations, and some aspects of nuclear C2 as well. So, the 25th has a lot on it's plate, a lot going on.

Now I couldn't talk about ISR if I didn't say a few words about RPAs, remotely piloted aircraft or what most of America calls drones. RPAs are an integral part of the

Air Force ISR, providing persistent actionable intelligence using unique platform sensor capabilities. Demand for RPAs, coupled with an ever-increasing requirement for ISR, have presented the United States Air Force with manpower and training challenges we are dedicated to improving them – it is going to take time, but we are making good progress.

Dedicated Airmen are using the available technology to effectively execute intelligence missions every single day. However, our method to update this technology is unable to keep pace with the growing demand for ISR, the rapid growth in data, and the changing nature of the global threat. So once again I say we must do better. We must do better with respect to agility to quickly absorb and field new applications to get the right data to the right user at the right time.

Now I mentioned a few minutes ago our Distributed Common Ground System (DCGS), this critical communications hub for collecting, processing, sharing and exploiting intelligence. This system was developed in the traditional acquisition lifecycle using block capability upgrades, which means, the capabilities took five to eight years to become operational… five to eight years, once again, not good enough, not fast enough. We have to do better. To overcome this challenge, we developed an Open Architecture DCGS Agile Framework and that is now what we are currently testing. This framework will cease all block upgrades with the goal of shifting average time to field new capability, such as analytic and cloud technologies, from what I told you earlier five-to-eight years bring it down to more like the vicinity of eight months. So that's the type of change that we need to do--we need to do much much more of it across the Department of Defense.

I'll close by saying that as I look around this room, I am just incredibly proud of what we've managed to accomplish together through collaborative relationships that we've fostered through our outstanding Airmen and our industry partners. At conferences like this we have a tendency to focus on things that aren't good enough, things that go wrong, challenges that we need to overcome, as well we should because we all need

to be problem solvers. Let's not lose fact of the magnificent Air Force that together we have created.

Now I've laid out some cyberspace and ISR challenges that we are facing in the Air Force; we would absolutely love to hear your ideas about how to overcome them. And together, together, I am sure that we will. Together I believe that we are well on our way toward a more integrated, networked, and multi-domain future in air, space, and cyberspace. Together, we're going to lead our Air Force, our military, and our country into the next generation of warfare dominance with information dominance at the core.

I want to thank you for all that you do. Please, please keep up the great work. Thanks so much for allowing me to be part of this important symposium. As I look around the room I see Airmen in uniform, I see civilian Airmen. I see retired Airmen. I see some in industry who are supporting our Airmen. To me you are Airmen one-in-all. So you know how I am going to end this, don't you?

Aim high Airmen, aim high. Thank you very much.

###