"Sustainment of STEM in the Workforce"

Dr. Mark Maybury
Chief Scientist, United States Air Force

AFA Air & Space Conference
National Harbor, Maryland
18 September 2012

[NOTE: Dr. Maybury was in and out of range of the microphone.]

Dr. Maybury: Thank you very much.

Can you hear me without the mike? I actually as a young man I was a disc jockey so I'm quite comfortable with all kinds of audio and video.

First of all, how many folks were at the dinner last night to see the Outstanding Airmen? If you didn't have a chance, I'm truly, truly humbled to stand before you. The Airmen who were recognized literally risked life and limb to deliver air power across the globe. I was just, just really amazed. I was driving home last night and just thinking about the kind of sacrifices they and their families made. So, to all of you who do that every day I thank you very much.

I'm in genuine appreciation of this because as the 33rd Chief Scientist of the Air Force I am not the first computer scientist to be Chief Scientist; I'm not even the first person from Massachusetts to be Chief Scientist; I'm also not the first Chief Scientist whose first name is Mark. In fact I'm Mark 33 because there was a Mark 31. I'm not even the first Chief Scientist who has a PHD in artificial intelligence. That actually was Ed Feigenbaum who is now Professor Emeritus at Stanford. I am, however, the first Chief Scientist who wore what many of you in the audience wear, who wore the uniform. I'm the first Chief Scientist who was a former officer in the Air Force.

As a young man my wife and I showed up at RAF Falconbury where I didn't know what a TR-1 was. As a Chief Scientist I got to fly a TR-1, one of the pleasures of the Chief Scientist. You do work hard, but you get to do some extraordinary things. I didn't really appreciate what that until I was actually in one. But it's also a great pleasure to be stationed in the Strategic Air Command for three years. We do have a great heritage and I'm really delighted to be a part of it.

The Secretary made reference, if you were a careful listener yesterday, to Cyber Vision 2025. Don't worry, for those of you who came for STEM, this is not a bait and switch. You are going to get the significance of STEM. However, I'm introducing you to essentially a sneak preview -- consider yourselves a small test audience -- because Cyber Vision 2025 will be released. However

we're releasing it first to our joint participants, to our joint partners, to our coalition, some of whom I was with this morning, as well as our other international partners, and to you. So you get to see it first, before the actual document is shared.

One of the reasons I'm sharing this with you is because it motivates very clearly, and I think compellingly why stem is so important. You heard General Shelton just talk about him not actually knowing of a domain in the Air Force that doesn't rely on space or air. And he actually went further and said I don't actually know of any military warfighter -- tactical or operational or strategic mission that doesn't rely on space and cyber. I actually believe that's true. I'm waiting for somebody to come up a nice example. I've not been able to find one.

We're going to split this stuff in two. We're going to talk a little bit about Cyber Vision 2025 and then we're going to switch into STEM.

Some of these slides are fairly dense -- hopefully not in the stupid sense of the word. But all of them will be available. I'll release them because there are a lot of good facts in here. Being a scientist I of course believe in facts.

So first we're going to talk about Cyber vision 2025. It's the second study my office has completed. The first one we did was in Energy Horizons. If you're interested in energy just Google Energy Horizons and you will find actually the full detailed document about how we intend to revolutionize the roughly $9 billion we spend on energy in the Air Force. It's actually just a little bit more than that. We spend about $100 million every year just in energy on our space enterprise, for example.

This study was focused on cyber in the near, mid and far term, particularly whether the Air Force should lead, follow or watch. Those were carefully chosen terms. The Air Force has done a whole bunch of things in cyber. We established a new career field and a new training program. Any cyber operators in the audience, just out of curiosity? I see a couple of hands. A couple of sort of semi-cyber guys. We also of course have our graduate program, Cyber 200 and 300 at AFIT. We have just, as of a few days ago, gotten those approved not only as joint courses but also importantly as courses that our allies can go to. So now the captain level and the major/lieutenant colonel level courses have now been opened up to our joint partners. We've just informed them of that actually. The first participants in those have been identified.

We also just graduated the first cyber weapons instructor course, and of course had the great honor of hosting Cyber Flag for U.S. Cyber Command at Nellis, taking advantage of the Air Force heritage of essentially not having any of our warriors experience combat for the first time in combat. We like to die 10 or 20 times first virtually, and practice, before we hit the battlefield. That kind of education and training that you heard the Chief talk about in terms of having great accessions, having great education and training and great capabilities. That triad is critical for high performance organizations and something that you'll see in here as well.

So Cyber Vision 2025 is a document, but more importantly it's a set of concepts and a blueprint for where we in the Air Force need to be going in the near, mid and far term]. In this form it's an unclassified document. It is primarily a defense document which is more operationally oriented. A document that's been formulated as Secret and low level intel. This particular document which is the real crux of the Cyber Vision focus was formulated in full concert and engagement with understanding the national doctrine engagement of our interagency partners, et cetera.

How do we do that? We engaged in a series of expert summits at Peterson, at Langley, at the Pentagon, with the National Laboratories, at all levels of classification. Obviously the topic is unclassified here, but all the way up to and including SCI compartment level via engagement of a series of experts. And we also issued an RFI. We got over 100 responses from industry and academia, from the National Labs, both in the classified and unclassified. So a whole variety of capabilities, and we learned a tremendous amount. I'll share just a little bit about that with you.

Then as a believer in the scientific method, believing that we don't have all the answers, we actually then put ourselves up against an independent expert review board which included a few experienced people like two former Directors of National Intelligence, former Directors of the National Security Agency, former CIA Director, former DIA Director, five former Chief Scientists, all of the members of the Air Force [Scientific] Advisory Board, and a bunch of cyber experts that I personally chose, having been a person who's worked for 30 years in computing, knowing most of the folks in this country and outside this country that have expertise. We hand-selected a series of folks to evaluate our homework and judge our homework.

So I think this particular document is a fairly well vetted, fairly solid activity importantly, and it also benefits from the steering committee for any of you who are inside the Beltway and

are familiar with the activities, in essence S&T planning that OSD's involved in. We actually directly connected this to the cyber priority steering activity. This vision builds upon, it actually extends that work that [Zach Lemnios] in the joint team created.

Interestingly, the document itself identifies the threat; the classified document obviously gets into a lot more detail of that. The document then focuses on cyber as a domain, because we need to do command and control of cyber. We need to do cyber battle damage assessment. We need to do cyber ISR. Cyber itself is a domain. Then we looked at air, space, command and control, and cyber as being functions that cut through all of the domains we operate in.

Then because the Secretary and Chief wanted to make sure I did my penance, when I asked them for a year to do the study they told me I had six months. I said thank you, sirs. By the way, we documented clearly what we'd have to do so I want you to include that on the S&T study. We want you to also look at acquisition. We also want you to look at test and evaluation, accessions, et cetera. And after they picked me up off the floor and resuscitated me and told me to get going I only have six months.

The good news is they gave me all the resources available. So we had operators involved in this, the undersecretary for science and technology, intelligence involved in this, the laboratories involved in this, et cetera. So we had all the resources we needed to actually put together this strategy.

So without further ado, first of all [it's a] threat. I apologize you can't see this in the back, but this is a depiction of the growth in everything from the amount of bandwidth, communications, the performance, the number of hosts, the number of users, the amount of money that is projected from FY12 out to 2025 in this domain.

One of the striking things, apart from the two billion more people we're going to have on the planet in 2025, the seven trillion IP-enabled devices that exist. That's one of my jobs is to advise and educate the leadership. By the way, they're much smarter than I am but nonetheless.

The point is that we're going to have exponential growth in a variety of areas. At one point one person said well is everything going up? I said no. Actually our best projection is by 2025 is the integrated circuit size will be around eight to ten nanometers, just to give you a sense -- today the state of the art in terms of Gates is about a million gates on a chip. To

give you a sense of that, the stuff that we had that General Shelton was just talking about, space tested capabilities, you're taking about 50,000 gates. So significant, a couple of orders of magnitude leap just in the past few years. Of course we project that to continue.

The other thing I'll note in terms of projection is that if you can see it, there's a red line and a blue line at the bottom. If you can't see it, don't worry. Trust me that next year the Chinese will produce as many PhDs in computer science as we do in the United States. If you think they don't produce quality, there are issues with corruption and other challenges that the Chinese system has in terms of their education system. I'll remind you that a number of those students are educated here in the United States. We can go into further details, but that's probably good enough for this discussion.

By 2025 there will be about a 2 to 1. About 8500 PhDs in computer science in China in contrast with our relatively flat line 3800 PhDs. So if any of you have children and you want to make sure they're going to have full employment, Dr. Maybury has done his STEM contribution. My wife and I have three beautiful children, one of whom is now fully employed, now going to grad school, and have a degree in computer science. As a sophomore in college he was hired in my home state which has a .5 percent unemployment rate in computing. The actual unemployment rates range from 8 to 10 percent just like the rest of the country. But that is an indicator not necessarily that my kids are really brilliant, but rather the issue of a lack of supply. This is going to become a strategic problem for our country in less than we take some action.

The good news is our second son is also Core 6 for any of you who know about MIT's courses, is a sophomore in double ECS. So he too, like his brother, is already getting approached by folks to hire him. Again, he's a great kid but he's just a kid. So we think this is indicative of the lack of supply.

We're working on our daughter. She's only 12. She wants to be a lawyer, so we're encouraging her to be a cyber lawyer, but we'll see. [Laughter].

The point is that this is not our design as parents. We were actually hoping we were going to get artists and historians and writers and the like. On the other hand, the good news is we know they're going to leave the house at some point.

The point is this is a strategic challenge for us as a nation.

I told you we talked to companies. We got over 100 responses to our RFIs both at the classified and unclassified level. Shockingly, the second most frequent category response was in mission support, meaning training people in cyber. Think STEM, continuing education. Actually this was a significant area of focus in these companies. We went to Silicon Valley, engaged with the National Laboratories. I've heard a lot of things. What I'd like to do is just quickly summarize three examples, just to give you a flavor of -- We don't have time here to talk about all the experiences we got through academia and the National Labs. But a couple were particular noteworthy. This was the only contribution I made to the study, being someone who has worked for several decades in this area, I knew a lot of the players, and I knew a lot of the history. So what I tried to focus on were some of the principles that we could extract that would be enduring not only ten years from now but frankly 50 years from now, 100 years from now. Much like, as we've all learned, the notions and principles of war, notions like surprise and massive force and so on. None of these principles have changed over time.

So what are those principles in cyber that we can similarly benefit from?

Limited privilege is a great example. My favorite example of this is the President of Akamai Technology. Has anybody heard of Akamai? Akamai is a company, a very successful global company headquartered in Cambridge Mass. He prides himself in saying that as the co-owner of the company he cannot shut down [his own system]. His system is a global caching system/. It allows you to rapidly deliver information around the world using a global support system. It is used throughout the DoD and commercial industry. What's interesting is that on the network and [Chinese] [inaudible]. There are trusted partnerships [inaudible] service providers. Neither can the cofounder of that company, nor the system administrator because he's limited his whole company, his policies, and this is one of the major ones, there are several others, which limits the amount of privilege that each one has.

The example I'd like to use to make this concrete is I as the Chief Scientist of the United States Air Force cannot install iTunes on my computer. Now my kids think that's ridiculous. What kind of technologist are you? You can't even use what's commercially available. That's a good thing. If I don't need it, why should I add and increase the attack surface on my space, increase the vector that an advisory can use on my machine if I don't need it. I can go out and I can buy a device, my own device, you know I carry two devices. I have a government devise. I have a personal device []. They're very wonderful. But I

don't necessarily have to have those two merged. So it was interesting when General Shelton was talking about disaggregation. I have disaggregation in my pocket. Now there's an additional cost, but the safety I get from that assures that the vector of attack comes from my children, I can separate from what happens in my business.

So hopefully someday we can do that virtually. We don't have to do that physically. Although, there are advantages to this physical diversity as well.

That brings me down to the second example, resilience. One of my favorite examples of diversity is AT&T, a great example automation. Twelve years ago that company created a command and control center, it manages ten percent of the internet traffic and has for the past decade throughout the United States. They had a significant event about seven years ago where the entire network went dark. Now not only did they not able to serve their customers, but their customers sued them because they were guaranteed services and then it affects the quality of their business. So, for the stock price of the service that's a significant corporate level event.

From that day forward [AT&T] established a new policy, they will never have more than one network device at one [main brain] company running the entire network. They decided they would never have more than a quarter of the network dedicated to one service provider.

Now, how much diversity do you need? Diversity has a whole bunch of benefits, not only resiliency but also has benefits for doing attribution or tracking down, doing real-time forensics. In addition that allow you to fight through. But that kind of diversity is an important aspect.

Another great example in industry is minimization. Microsoft for the first time in the history of the corporation, their next OS which runs on Ismoto is actually smaller than the previous OS system. It's always been in a stage of growing. Now the motivation for them doing it is to run on small devises, but from our perspective, small is beautiful. Small means, in our Air Force sense, less dependency, less attack surface, less potential unexpected complexity. So all these principles were illustrated through multiple organizations that we heard from. I think that's partly what we need to do as a service; understand these principles, translate into acquisition activities or operational activities if not technology investments to improve our resilience.

So a couple of other slides and then we'll get to STEM.

The findings of the study include some things you've already heard. We are critically dependent upon cyber, just as we're dependent upon space. Cyberspace is presently contested or denied. Where we've been denied, we can talk about area denial, lack of freedom of movement, lack of ability to get into an area, anti-access. The same is true actually in cyber. There are parts of the world where there are entities that govern those networks don't want this evolved, don't want this access. That might include access in our own space.

Research will be constrained. People particularly talk about sequestration and money. But I'm here to tell you that money is not everything. If you had told me I could choose time, treasure or talent, I'd have a big argument about time versus talent, but I wouldn't really argue about money. That's a little bit counter-intuitive. The point is all are important, but we cannot even attempt -- Those PhDs we talked about before, they take eight years at minimum to produce. A long timeline. We talk about system time lags, but if you think of the human system, that's a significant limitation right now.

Finally, we've gone beyond the virtual realm to the kinetic realm. You all know about Flame, we've all heard about StuxNet. It's the case that now cyber effects have become Physical. I like to joke, one of the things we've heard in Silicon Valley, everybody talked about bring your own device. Basically Silicon Valley several years ago gave up barring people from bringing their own devices to work. They basically said we can't stop people, so they accepted it and started building security features to allow the integration of devices.

Just imagine what it would be in the future when we tell somebody you can't bring your own devices to work when those devices are them.

Memory devices, perceptual enhancement devices, cognitive enhancement devices. These are not matters of science fiction any more. These are now matters of active science.

So it challenges us in terms of thinking about the kinds of controls we might have over technology proliferation in the future.

Cyber Vision 2025 then found our missions are at risk because of some of the things I've been talking about. Inter-dependencies, growth and complexities. Just a couple of examples on the bottom there, our F-4s, we hear a lot of air power heritage here. Only about 5 percent of the F-4 depended upon any

kind of software. Today's F-35s, to just start the aircraft you need to have the automatic logistics system, ALIS, which is a 50 million line code system connected to the aircraft which is on board.

So it's interesting. Microsoft is reducing their attack surface and we are, from a cyber perspective, increasing our attack surface.

Now to be sure, propulsion is important, weapons are important, TTP's are important and the like. So air power hasn't fundamentally changed other than the actual relative mixture of physical and virtual has changed significantly in the past 10-20 years.

No different in space. In space here, I left off [inaudible]. Put [inaudible] on, and immediately you're talking about the kind of code that [inaudible]. As an example, I was a grad student at Cambridge, affiliated with the RQ1 Reconnaissance organization. We were building essentially the predecessors of video signal processors for speech recognition, signals intelligence that operate semi automatically. Today that actually exists in this phone. We had super computers we did our science experiments on in grad school. Today they are in my pocket.

The capacity for us to predict the future is I think challenging. Yet cyber S&T can give us appropriately employed assurance, efficiencies, can give us also resilience in some of the ways I've talked about. Partnerships can be important.

Our vision for cyber from science and technology is assured cyber advantage across all of the mission domains for the kinds of things that we seek here in terms of agility, resiliency, and an effectiveness edge over adversaries. And we came up with a set of recommendations including assurety and power in the mission, which includes more effective integration of [inaudible], but also frankly, we need to certify and accredit our mission systems to a much higher level of assurance in our business. It's important to all of us to have appropriate medical records, digitally. It's important for us to get our checks at the end of the month. But in the final analysis if we can't assure command and control systems. If we can't assure space effects because of cyber vulnerability, we've really done a disservice to the nation.

So assurance of those national security systems is a focus, is a current focus and will be a sustained focus.

We also increase the cost of the adversary's operations; make it much more expensive for them.

A great specific example, if there are any Airmen who spend time overseas, particularly our Pilots, have this experience and all of us in a foreign country have had this experience. You may need to communicate back home. So what we've produced is a little disk, our laboratories have a little disk with about a 79,000 line code operating system, a secure LINUX operating system. It's got a little virtual private network in a little especially carefully selected PDF reader. We have this for our pilots or our Airmen who go overseas. You take that disk, say you're in a hotel and they've got a log-in to submit your flight plan with [IKAO]. They go down; they can plug that disk in, boot the power, and reboot that machine on that trusted disk. Now it's not perfect. Some adversary who is very sophisticated can figure out ways around that, but for the vast majority of cases, it's going to be more than sufficient to be able to operate from someone else's untrusted platform in a trusted fashion. That will significantly, it's an example of how you can significantly increase the cost of the adversary's operations with a very very simple fix.

Improving cyber education is really important. We'll come back to this in terms of STEM, so I won't focus on that.

We also want to make our acquisition processes include security up front, include test and evaluation up front, and have more rapid iterative, open acquisitions. Then you've heard General Shelton also mention the importance of integrating across the board function mater plans. Because cyber is so embedded in our airspace, command and control, global ISR activities, it's going to be critical for us to ensure that we have effective integration across those.

We're also going to have to reduce the complexity in our systems, come up with new methods of verifying and validating our systems, because we depend on them. I mentioned the F-35 before. It is the state of the art today with about a million lines of code. So you can see our systems have exceeded our ability to actually do verification and validation. It will only get more complicated as we add machine learning, artificial intelligence, and other kinds of non-linear effects in our systems.

The only thing we can do, you heard General Shelton talk about agility and resiliency and disaggregated architectures separating physically and functionally. You can do that in space, you can do that in cyber. Also we have machines for improving our situation awareness. It is a great gap area and a great technology opportunity. It's not only mapping our networks but also mapping the missions that operate on those networks. Today we do that manually with our Predator/Reaper operations.

Right now we manually look at all the hundreds of connections and dependencies in terms of com and networking that those missions rely upon. We want to be able to do that automatically in the future. There are ways in which technology can help in a fairly straightforward way.

The last recommendation is focus on enabling science and technology. This will lead into now STEM, the importance of STEM. We've identified four major areas, not only sharing but also empowering the mission using cyber to actually be a force multiplier, whether is actually be a DCGS or in terms of onboard processing and sensor platform that optimize human machine systems. This is an area where we've gone beyond the recommendations of agility, resiliency and assurance in the under-secretary of defense's strategy. We've actually added the human dimension. Knowing how important the Airmen are and all the services contributions are to cyber we can't just think about just making faster computers and more sophisticated connectivity. We also need to think about training. We also have to think about the symbiotic integration so that as machines are processing, right now the processing speed of our best systems today, which by the way the advisory can use to get into that system if they can be faster. We need our Airmen who obviously don't operate at that speed, maybe perceptually, but not commonly. How do we bridge that gap? Make the Airmen aware and the systems transparency and also similarly allow those Airmen to be either on the loop or in the loop when necessary. Or frankly out of the loop when appropriate.

Finally, foundations of software and hardware trust. This is an eye chart. You can have it, take a look at it at your leisure. But just to share with you that across each of these areas in our vision, for ensuring and empowering, for enhancing agility, resilience and so on, in the near, mid and far, we've identified where the Air Force needs to be a leader, a follower and/or a watcher. So that's a signal to -- We've had conversations with our other service partners, international partners, but these are areas where we, the Air Force, must lead.

This is going to be particularly important for us as we go forward in the more fiscally and human and time constraints. When I say time constraints, it's not just that 25 milliseconds, it's the evolution of the threat. Technology is changing very rapidly, but the threat is changing very rapidly as well. That conversation can be very explosive. It's our ability to do, for example, real-time forensics will be very important for us. Attribution, you heard General Shelton talk about it. Another great challenge in this domain.

I think in the end perhaps it's not insoluble, but it's present beyond the state of the art. These are the kinds of areas that science and technology need to work on.

We can't do this alone. You heard General Shelton say we don't have enough people in the world, enough money in the world to do it, so we're going to have to partner, and all of these people are folks we've been engaging with from DARPA to international participants to national labs.

In short, Cyber Vision 2025 is the vision for the assured cyberspace advantage. A principled approach will help us, we believe, achieve these effects. But as you heard the Chief say before, innovation, Airmen innovating, will be very important in this area. Our partners as well.

What I'd like to do is take a few minutes on STEM. Obviously we can't achieve any of these visions, whether they are visions in cyber, space or air without STEM.

You can see a couple of quotes here which I won't read. But from the President all the way down to our current Chief articulating the criticality of STEM. Our Air Force is a service whose DNA is science and technology.

We are mechanical flight. That is our origin and in my opinion our future. So how we advance that and how we control, if you will, how we dominate in the science and technology space and translate the operation will be decisive.

We have a great not only legacy but current experience. General [inaudible] had a chance to go downstairs and meet one of these individuals. Actually Matt Squires. If you have a chance, go over to the laboratory. You will meet a young American science hero. I can't make this stuff up. One of 96 presidentially recognized, the only Air Force and maybe in the service recognized. But Matt literally, and you can see it in the physical device, both in terms of free and controlled [cold atoms]. We expect to actually have a prototype by FY13 of this technology. If anyone hasn't been exposed to [cold atoms] this is one of the methods that will help us fight through denial of GPS. Basically by looking at the location, entering the timing moment of laser cooled to reduce the thermo effects of motion at the atomic level and using that in a fairly compact package. . You can actually go downstairs and see one of the packages. I encourage you to do that. More importantly, meet Matt and you can blame Dr. for sending you to them. He is really an extraordinary young American and very down to earth.

Laura Barnes, Lieutenant Colonel Laura Barnes, another amazing Airman. She was the first ever non-UK citizen to be recognized for her work in directed energy. She went to the UK Defense S&T Laboratory where they gave her a medal for being able to educate British defense science and technology leadership and scientists on how directed energy will affect humans. I can tell you we know a lot of this. The Chief Scientist has actually been shocked by a microwave and I'm so comfortable with it that I'm going back again next month.

But nonetheless, the point is that our science is excellent, it is world class in directed energy. So you can be very proud of our leadership. We literally have Nobel Laureate level talent.

However, that's the good news but there's the bad news. I don't want to leave on a completely depressing note, but you've got to know the truth. We're fifteenth, some say sixteenth in science and technology [inaudible] in the world. It's the case that our reading, our mathematics numbers. You can see the comparison there in terms of indicators, National Science Board indicators. Japan versus the U.S. and China. You can read the statistics here. The good news is we're spending about $40 million a year in explicit S&T [outreach] not only to universities, but more importantly the high schools and even before then, getting our kids at the 6th, 7th, 8th grade. Even, frankly, before then if we can. This is critical for the future.

The good news is we have a significant representation in our Air Force of STEM degree folks. The Air Force Community College has awarded more than 335,000 applied science degrees. The Air Force Institute of Technology, 16,000 STEM graduate degrees. Forty hours of required STEM work at our Academy. So we have a strong corporate commitment to STEM development in our forces. Again, some of the stats. Nonetheless, we're lagging in production. You can see us down there. Way down at the bottom of this in terms of our 24 year olds, in their prime, in terms of actually having STEM degrees.

You can also see here the kind of cognitive level comparison. Asia versus Europe versus the U.S. When you go to the U.S. it's about one-third STEM, two-thirds non-sciences. Go to Europe, it's more equal. You go to Asia, it's just the opposite.

One of the points I like to make is that STEM, and I love social science. I really do. My sister is a psychologist. I took psychology. I have an undergraduate degree [inaudible]. So I love the arts. I'm a musician. However, [manufacturing] capability yields wealth yields military power. So I think we have to be attentive to the strategic import of STEM. Not just

on having smart people but also having a robust economic equation and a robust military capability.

The good news is we've been doing better in the last couple of years since 2001, actually raising our percentages of accessions with STEM degrees. It's still not as high as I'd like to have it be. In the technology service I'd like to have it be more like 70 percent. But we need doctors, lawyers, [inaudible], chaplains, we need all [inaudible] as well, but we also need the capacity to do what we do best, which is [inaudible] science and technology in air, space and cyber.

The better news is that our general officers, even though we have [inaudible] minorities in STEM degrees in our general Air Force population, in our general officers over time, since way back in '47, Hap Arnold's time, you can see actually the growth of especially general officers with undergraduate degrees.

So that's really [inaudible] the services value. You can argue value, but [inaudible]. I think it's because [inaudible] smart, but you may disagree. But at least [inaudible] more successful for whatever reason. Now a degree shouldn't secure a promotion in the future, but I do think having critical thinking of understanding data and analytics is an important aspect of success.

So we in the Air Force have a variety of initiatives in STEM. The Air Force National Research Conference to study recommendations including the establishment of an Air Force wide STEM Advisory Council which I sit on which is chaired by General Davis. That Council has published objectives for STEM. We've established STEM outreach office which actually been supported a number of activities represented on the next slide.

We have studied looking at actually all of our STEM disciplines. We do have an issue; we need to get better at articulating our STEM requirements so we have some work to do there. So, I have been encouraged and as you just saw in Cyber Vision 2025, just as an example, is an illustration of the importance of [human capital].

Here we see [inaudible], the AQR, actually the Outreach Coordination Office Director. If you're involved in STEM activity or your base is and/or you'd like to be connected, he's a great individual to connect up to. As you can see here, [inaudible] point of contact, developing an annual plan, acting as a clearinghouse for STEM activities.

Just an illustration of some of the activities, at 20 Air Force locations, hundreds of schools, thousands of teachers, 1500

Air Force scientist volunteers. I myself have personally mentored one of our outreach activities her. As well as our Vice Chief. This is how important this is to us. This is not a nice to have. This is not an additional duty. If we do not do this we will not be the Air Force of the future that we were in the past. That's how important this is.

A variety of partnerships as well. We have a great partnership with AFA. In fact we have three new teams here in the Cyber Patriot activity. Obviously I'm passionate about cyber. That's one of my biases. But the good news is we've got now [inaudible] Hanscom three new teams for FY13. A great connection to Civil Air Patrol, STEM outreach program as well. Cyber Patriot had a great activity.

Interestingly, that's at the high school level. At the collegiate level the Air Force Academy won the collegiate level cyber competition and then went off and placed number two in the national competition. So we have some really amazing cyber warriors. Again, ultimately finding deep roots in some of these activities.

In conclusion, I've told you a little bit about Cyber Vision 2025.

I just want to leave you with ten final thoughts. I've already mentioned the first one that our foundation, our roots are really in S&T. That is the history of the Air Force.

It is also the case that even now, and more so in the future, our success will be critically dependent, critically dependent. It will not be a substitute. We're not going to create a new human life form that's going to make us somehow magically more productive. Those productivity capabilities have and always will come in science and technology.

S&T provides [inaudible] investment productivity and operational efficiencies. We do these faster, more effectively and more successfully.

There always is a tension between where money should go now and in the future. You should know that your Air Force leadership has been very aggressive at protecting the STEM seed corp. They've done a really good job at that. That is our sustained plan for the future.

Basic research is long term. S&T [inaudible] requires years to develop and there is significant development. Just some examples-- stealth, global positioning, remote operation. More and more we're seeing increased [inaudible]. [Inaudible].

It's [inaudible].

Finally, it will require us to sustain the commitment. These aren't things that happen overnight. The reason we have cold atoms downstairs in the demonstration booth. We have a presidential recognized researcher that we recognize S&T [inaudible] in the Air Force, a commitment to science.

With that, I thank all of you for all that you've done for S&T. I look forward to partnering with folks and I'm happy to open it up to any questions.

Question: What do you think are the consequences of our just flat STEM production in the United States compared to across the world? What are the implications and consequences?

Dr. Maybury: I think one can always learn to do more with less, so just because [inaudible] doesn't mean you're using that [inaudible] for the most productive and important [inaudible]. Hence [inaudible]. My office has identified [inaudible]. There are some areas where we don't need [inaudible]. [Inaudible]. So prioritization will be very important. If you're going to have a flat production you're going to have to decide [inaudible].

The other thing is from a macroeconomic perspective, from a strategic military, national security perspective, you have to almost look at the system to see whether or not you're producing the effect that you want to achieve. In the end, what does S&T give you? It gives you a variety of outputs. It doesn't just give you science. It also gives you military capability [inaudible]. So it's a whole variety of, if you will implications for [inaudible].

To answer the question perhaps another way, all of the world is studying America. [Inaudible]. S&T centers of [inaudible] popping up in Beijing and Bangalore and on the African continent now. So this is, they are students of what has worked economically [inaudible]. And the fact that they're replicating what we're doing ought to be a signal for us.

# # # #