Program Transcript

Plenary Session #1:
A Conversation with Mr. Tom Bossert

Walter E. Washington Convention Center, Washington, D.C.

Wednesday, September 6, 2017

This transcript has been edited slightly for brevity and clarity.

Participants

- **Tom Bossert**, Assistant to the President for Homeland Security and Counterterrorism, National Security Council, Executive Office of the President
- **L. Roger Mason, Jr., Ph.D.**, Senior Vice President, National Security and Intelligence, Noblis (moderator)

Roger Mason (RM): Thank you very much Chuck [Alsup, INSA President] and good morning to all of you. I'm delighted to be here and I just can't think of a better way to set the tone and tenor for the next two days than having our opening speaker, Mr. Tom Bossert. He's known to all of you, but let me just recap a little bit of his very distinguished career. Currently, the President's Homeland Security Advisor, but prior to that he's had a very distinguished career in government to include time at FEMA, time at the Office of the Special Counsel, time as Director of Infrastructure Protection, and also time as the Deputy Director for the Homeland Security Advisor under then President George W. Bush. He holds a B.A. in Economics from the University of Pittsburgh and a law degree from the George Washington University, so please join me in welcoming and thanking Mr. Tom Bossert for joining us this morning.

Tom Bossert (TB): Thank you.

RM: So Tom what we'd like to do is actually have you start off telling us a little bit about what's on your mind and your plate this morning.

TB: Roger, thank you. Chuck, thank you. [INSA Chairman] Tish Long and [AFCEA President and CEO] Bob Shea, Jake Jacoby, really thank you for inviting me and thank you to this august group. For me to be the one to control your schedules is a first in my career, so thank you for that. It also feels a little like an interrogation so well staged for the intelligence community; I can't see you but the bright lights here allow me to only tell the truth, so I think that's the idea.

Couple of things, I guess to answer your question. Outside of the intelligence world, what's on my mind this morning is on the television of most Americans today, and that is Hurricane Irma, so before we get into the intelligence and fun stuff, let's get into the really scary stuff and that is the crisis upon us. I thought we just, and I'm gonna say this with some background and knowledge to say it, pulled off the best, well-integrated, fully-integrated operational response at a federal, state, and local level in our nation's history in responding to Hurricane Harvey in Texas and I think that that's based in fact, not just anecdote. And then we got 24 hours rest and we are waiting for Irma. So that was something that struck me on the way over here, was forecast. And so, perhaps a lesson here in an intelligence-led planning. We had not just the forecast of the storm but the NOAA folks this year forecast as a modeling matter that this would be an above-normal and dangerous hurricane season, so there you go: we should listen to our modeling and forecasts.

Irma is probably hitting the U.S. Virgin Islands and Puerto Rico right now as we sit here, that's on my mind and it is forecast to hit Florida and cause a lot of damage, so that's on my mind this morning but it is not the only thing on my mind as you are very important to me, the counterterrorism mission is very important to me, the cybersecurity mission is forefront on my mind most days, and it strikes me that all of these are functional responsibilities, and they're all downside risks so that's what I do for a living and that's what I'm here to talk about so I appreciate the invite. We'll give you an Irma update before I leave.

RM: Great, thank you very much. We know your time is very valuable and the enormity of your schedule so let's jump right in with some content. You sit at a unique vantage point, at the intersection of homeland security, cybersecurity, and intelligence, and so the question is one of the instruments providing the intelligence that's needed to do that job is the [Foreign Intelligence Surveillance Act] FISA Amendments Act, first done in 2008 after 40 years of the FISA act, reauthorized in 2012 but its sunsets this December. What's the impact? How important is the FISA Act, particularly the 702 provision with respect to your job and the larger homeland security apparatus?

TB: I can give you the talking point first and that is that the terrorist threat is not going to sunset, and so the authority shouldn't either, but that's a little glib so let me give you a better answer. If I can, let me take

a step back. So I try to look at this from the strategic perspective of what it is we're doing and how we're going to continue to do it as a society and what we did nine years ago, nine and a half years ago, was modernize an otherwise fine law that required us to do things that we couldn't do anymore for practical reasons, and that is to adapt to an app-driven—Chuck mentioned there's even an app for this conference— Internet-connected world.

The idea at the time was that we can't continue to pursue, as you in this room know, individual court orders against foreign adversaries with foreign intelligence value in foreign lands who might happen to choose, understandably so because it's superior in class and performance, a U.S. Internet service provider, backbone, or a U.S.-developed app, or a Google storage platform. The idea of a foreign terrorist in a foreign land using Gmail was a novel concept in 1976, it's obviously a prevalent practice today, and so what we have to do is think about this in the context of lawful access to information. And I know that is sometimes viewed as a code word to some about encryption and other things; that's not the intent. Call it lawful collection of information but whatever you call it, the idea of cybersecurity and 702 authority, and even, I don't know if he's here but Paddy McGuinness, my fine friend from the United Kingdom, thank you Paddy for being here, he is a leader that deserves a lot of credit for encouraging me and the administration to do the right thing on U.S.-U.K. data sharing and I'll talk about that here in a moment. It is currently President Trump's position that we should pass legislation on the Hill, and I believe Paddy McGuinness stands as the first-ever foreign official to have testified to both our House and Senate on legislation that the U.S. wants, or maybe on any legislation, so thanks for being here Paddy. But all three of these things are connected. The idea being that we now have to, unless that law is passed, go through a long and slow process wherein a foreign court has to request of our U.S. companies compliance with a foreign court order, that takes a long time for those of you that are familiar with the process, and in the interim we end up with criminals, terrorists and other malefactors languishing or getting away in some instances and that's not acceptable.

There's a much easier, and faster way. We're pursuing that but it all has to do with modernizing our means and methods of transferring data and allowing access not only to our government, to our data, and our companies' data but foreign governments that are trusted with certain rules. Back to 702, to me 702 is probably one of those things that should have sunset so that Congress could review it. I concede that, but now that we've gone through nine years of bipartisan use and demonstrated value, this Congress should be exceedingly pleased with how it has been implemented and how it has protected the U.S. people against those abuses that they foresaw. Fortunately, they should be proud of it and they should reauthorize it. Unfortunately, that's going to require us to reeducate some members that weren't here at the time, to educate the public on what we do as an intelligence community and to ensure them that we have some trustworthy mechanism in place that will allow them to have trust in their government institutions and I'm here to do that. I'll speak to the details of it, but I want to make sure you think about this from a strategic perspective: why is that we need to have a separate standing section of law that allows us to – I think we're the only country in the world that has such a thing – that allows us to provide this protection, in some cases even to foreigners that have intelligence value for us? Right now that information is arbitrarily cabined off by jurisdictional boundary and what I'll do is that today for those of you in the intelligence community, I'll offer you a challenge as we move forward, and that challenge is for us to determine ways to better mission integrate by function as opposed to mission integrating by geography.

I've inherited a world in which we still have regional directors on the [National Security Council] NSC staff; I think that's a valuable thing. We have a Russia desk, a China desk, and so on. That's a world that we have lived in since World War II. When the homeland security council was invented, I had the privilege of serving in it and on it on the staff, the idea was to develop functional directorates—cybersecurity, a transnational issue; counterterrorism, a transnational issue; even homeland security exceeds our borders and parameters, it's not a western hemisphere desk, it's a homeland security function, and so the idea here of data existing in a server in Seattle and being relevant to a terrorism prosecution of a British citizen in London, having to wait for a year while process is ironed out is not an acceptable outcome. And so Paddy and I are working together and have now proposed on both sides of the pond that we engage in a new world order in which that happens much more quickly. Once the Attorney General certifies that that other country has the right principles of law to protect that thing that we consider our American values, then we can establish a more trusted relationship in the executive branch. That will happen, and once we

provide that information in a more efficient manner then companies like Microsoft and others won't have to decide where to house their repository data and develop artificial business models. Instead, they'll be able to sell a [Microsoft] 365 account with surety to a British citizen and keep that data wherever it's most relevant.

So, that takes me back to 702. 702 is an authority that allows the U.S. government to collect foreign information from foreigners—non-U.S. citizens—on foreign land. It doesn't allow collection against U.S. citizens; we can't target them. It doesn't allow collection on a foreigner that's here in the United States and so there's a whole lot of misnomer around this authority. I'll clarify it within Q&A but as you think about it in 10, 15 years with technologies like Blockchain and other things that are emerging, think about how increasingly odd it will sound to our grandchildren that we had to have a conversation about where the data was stored and what sign post it touched as it went through an efficiently organized internet, and then come back to this conversation and watch it. They'll probably watch it on a device we can't conceive of, but let me stop there and we'll go back to 702 later.

RM: Great, that's a terrific, fulsome answer that I'm sure the audience appreciated for sure. You mentioned the topic cybersecurity several times and obviously none of us can go through our daily lives without hearing about a breach of some magnitude and if you look back to some of the big ones—Sony, Sands Casino, OPM and others, what's striking is, you know, with really garden-variety tactics, nation states or other organizations can achieve strategic effects through cyber, from that perspective. When you think about what we need to do as a consolidated, national security enterprise, combining cyber threat intelligence with the network defenders, and adding strategic context in terms of the 'why': what's your sense in terms of how are we doing with respect to first of all with all that integration, and second of all, are there some things that we need to do or could do more to help that? For example, there have been some who've advocated creating an NCTC, National Counterterrorism Center-like entity for cyber across the government. That's got pros and cons, obviously. I think the audience would be interested in hearing your reaction to that topic.

TB: Yeah. Broad topic, narrow question. Let me see if I can answer it in reverse. Here's the answer, and it may be a timely answer on the organizational construct. I'm now President Trump's homeland security and counterterrorism advisor, I have an obligation and responsibility to make the current construct work and work well. First, you don't have to be bad to get better. For anyone that takes my observations about improvement as an indictment of their current performance: do not do so. We have an opportunity now to take the construct of the Department of Homeland Security's cyber mission and improve upon it. I think it deserves a lot of credit for that, which it has done, I think it deserves a lot of support as it tries to improve, and I think it needs to improve in capacity, in arms and legs.

But I also think that there's some authorities issues that we're going to have to discuss; I don't want to get too far in front of our cyber strategy as we roll that out, but the idea here again takes me back to our friends in Great Britain. There are two constructs here, we've got an Israeli model and a British model, both of which have demonstrated some success, but it is misunderstood in the following way: there's an organizational construct and there's an authority construct. I'd rather focus on what it is we'd like this entity to do and not where we want to house it. The idea now is that we've got DHS, it is functional, it is working, and it requires the love and attention and care of appropriators and authorizers to make it better if it requires improvement. I believe it does, but not because it is performing badly but because it could do better in terms of a defined mission. That's the answer on organizational construct, I want to make sure I'm clear on that: we don't need to create an NCTC model. If, in a year and a half's time, we've still failed to produce results I anticipate that that will be the public debate and we will end up having to do something of that nature just to bring the attention it requires to the subject. However, I'm here to bring that attention without an organizational construct. We have DHS, we're going to make it work.

Now, let's talk about the authorities, that's the bigger question. This is the tough one. How do we, in our own national interest, continue to be dominant in and able to collect on what we all refer to as SIGINT, but collecting information on the Internet against our adversaries in a way that informs our policymakers and decision makers, while also behaving within a set of norms that allow the regular citizenry to conduct commerce and communicate to one another. I think the answer to that is a little bit more obvious to Americans than the rest of the world because we impose our own values on it, but what I'd like to see in

the future is a world in which we have that kind of common agreement among our like-minded allies and that we not only have norms but we enforce them. Now this is going to look a little bit like a law enforcement, criminal matter, in other words, cybersecurity is a little bit misunderstood it's more about cyber risk management. We will never have a world in which it's an inherently and completely safe Internet, in my view, at least to my current understanding of the technology. But what we will have is an opportunity to clearly take those who offend the law and punish them.

TB: So that's going to require three or four things – start with an attribution standard, it's going to start with agreement upon certain bedrock norms of behavior, what we will and won't do. And it's going to start with a requirement we have allies in that and for right now I love multilateral bodies for a lot of reasons, and for establishing norms, they're very beneficial. But I don't always love multilateral bodies for the purpose of enforcement. They have different political agendas and they have different group dynamics that don't allow for the individual defense of the United States, let's say, in this instance. So what I hope to do, is role out in a way that increases our defenses—because I do not believe that any other adversary will just stop and behave because we tell them to—and those defenses have to, not only be a shared responsibility with local authorities and individuals, but they have to require us to improve our capabilities and capacities at DHS, and so that's something that we'll promote.

I would stop right now because Congress is back in session, instead of cajoling them like I'll do on 702, I'd like to thank them for giving us more money on this mission. We're going to get more money from this year. We're going to get more money from them next year, it's necessary. The collective defense is going to require a political conversation in this country about how much we want to trust our government entities to defend our networks, and at what level. That will be, maybe, a little bit of a vailed conversation, but it strikes me that I'm talking to you, the Intelligence Community, here in the room, but there's also cameras in the back that might capture this for the rest of the American public, so I want to make sure I keep it at the right level.

The last illusion I'll make here on cyber is to the need to take those countries that have an asymmetric advantage over our companies, and to remind them again that if they haven't already agreed with us to stop that behavior, that we won't tolerate them using their government capabilities and their intelligence collection capabilities, which are strong and well funded, to collect against our individual, profit-making companies like Coca-Cola or the DNC for that matter, any user with dot-com. That's something we can't tolerate and that's something they've pledged to not do especially as it relates to stealing commercial information for their own company's benefits. I'm pleased that the last administration in a bipartisan way here, attained that relationship with China and those agreements. But they were non-binding, so we want to remind the Chinese to make sure that they remain within the spirit of that agreement. If we see in the evidence that they're not, we will call them on it. In the interim, that's what we'll continue to do. At the end of the day, we'll improve the authorities to defend a little bit more greatly.

RM: Terrific. Let me follow up on an earlier statement, insertion, that you made, which is an interesting one and an important one. When you look at the post-9/11 world where we've spent a lot of time as a national security community integrating the piece parts, and in particular again, you've got that unique vantage point, where we've gotten to integrate the Intelligence Community with federal law enforcement and homeland security. You mentioned early on that the emphasis would be on cross-functional missions as opposed to regions. First of all, what is your sense in terms of the state of integration, post 9/11 since you've been involved in this since its birth after 9/11? What's an example of a cross-functional mission that we can really spend some time and effort on to move the needle, so to speak.

TB: The state of our community is better and stronger, I think that's a given, and that goes across the board. So from a prevention perspective, all the way through to the response perspective I mentioned at the outset here. The two things that struck me the most in the transition back, it's kind of a constant state of comparative analysis I'm engaged in. I've joked that I'm literally back in the same office suite, and it took me 10 years to get promoted ten feet. From the vantage point I hold now, and the vantage point I held then, as the deputy homeland security advisor, three things have happened.

First, the world has become increasingly complex in terms of its interconnectivity, the questions that are more difficult, transcend boundaries and become transnational. Second, the threat has become more acute and widespread at the same time, at the same time; those are two different things. We were using the AUMF when I left, it's almost nostalgic, in two countries. Now we're using the AUMF [Authorization for Use of Military Force] in more. And now we've got upwards of 17 or 18 nation states that might be failed or viewed as close to failing and they have strong presence of either ISIS or Al-Qaeda or other groups or all three. That is a troubling development. For the last eight years, we've done a nice job at keeping the leadership at bay. Some people have gruesomely referred to that as "weeding" or "mowing the lawn". I don't like that term. But if you if you take that analogy, while we've taken the large leadership weeds out of that analogy, we've seen the lawn spread. And so from a counterterrorism perspective, I'm alarmed at the spreading of the ideology and of the groups' presence into other ungoverned spaces and that is just the counterterrorism threat. The growth of the cyber threat, we just covered, it's trending in the wrong direction. It's why we have an urgent need for an increased defense as a country. There's nothing defensive about that. I'll explain that more in a bit. We need a greater ability to defend against an inherently vulnerable technology problem right now. Thirdly, what strikes me, is that institutions have matured, as we have envisioned, and that's encouraging, but some of the holders of the positions, have not. So we all go through institutional turnover, some of the leadership of this organization here in the front row have long distinguished careers and now unfortunately have left us. So while there is a new crowd of leaders, the feeder pool of staff, have in some cases, and I'll pick on the young man that came here with me today, don't really recall 9/11. That struck me as profound, as I walked into my office. There is a generation of Americans now that view 9/11 in the way that I might have viewed Pearl Harbor. It was historic, it was understandably profound, but it seemed distant, and it seemed like something that might not happen again until you grow up and realize it does, and will, and can.

I guess I would take a little bit of a plug to not only mission integrate by function, which is something of a little bit of a mouthful to those of you that work multi-agency, multi-jurisdictional world, and that needs some improvement. That's the second time I've mentioned it; I'll say it a third time before I leave this stage. I am a little bit dismayed in our inability to mature more quickly through those jurisdictional and agency boundaries. This, maybe, is a counter-narcotics example, to take me out of terrorism, or a human trafficking example. We in the intelligence world tend to focus on intelligence for the PDB [President's Daily Brief] every morning. We also tend to focus on intelligence that will inform an operator. It is the intelligence that informs an operator that could be better integrated in the mission and function. At DHS, I know David Glawe is there now and he's going to do a great job at advancing this. It's not just a terrorist threat. He's going to increase that intelligence-led policing and sharing mission in a way that then informs customs and border control, the immigration customs enforcement. The Mexican and South American partners that we have are going to share their information with us, and us conversely with them to address the pernicious problem of transnational crime and drug-related crime. Those types of things require intelligence to inform policing activity. And that's what I mean by mission and function integration. That's the example to give you.

RM: It's a good one.

TB: Let me leave with the people here. I set up that the people are the shortcoming. Goldwater-Nichols had a great solution to this. I think perhaps the authors of it thought they were going to make it a better class of flag officer. And they require, for those of you that don't know here, that you have some degree of joint operational experience, training, and education as a prerequisite to promotion. We're going to have this great class of flag officer. Instead, what we got, was something better. We got a much better feeder pool of candidates that increased and bettered the readiness posture of our entire military. What I'd like to start doing is thinking about how to do that across not just our intelligence community as narrowly defined, but across a wider scope, defining it to include law enforcement, international and domestic partners. If we have a by-with-and-through strategy on counterterrorism, then we have to think through the challenges of a federated information gathering and sharing model. If that is the case, then we're going to have to rethink through some of our rules gathering intelligence sharing, as most of you in the room know. If we have an intelligence based, broader scope professional development program, we won't just have a better class of SES candidates, we'll have a better feeder pool. I'll give you my two cents on the distinction between these two things. If you can get somebody to spend a year or two in the shoes of

a consumer of the intelligence that they collect and analyze, they'll be a better collector and a better analyst. If you can then train them, and the difference between training and education is that you educate to innovate. You train to replicate. When you train them, you train them to replicate a process or procedure or function. When you educate them you open their horizon, you open their mind. So what I'd like to do, for those of you that are leaders in our government space right now, is encourage you to start allowing your best and brightest to leave you; I know that's counterintuitive, but do it in a way that's looking at the future of their careers. Start cultivating them. I joke about the same young man that I criticized not remembering 9/11, I also tell him he's going to be the next CIA director. It's just going to take him 30 years to get there. So let's see if we can think about our professional development as we think about our mission integration. That would be the three things that I have seen: more threat, more complexity and a waning memory, I guess, in our workforce.

RM: That's terrific. I know on that last topic in terms of human capital, I speak for a lot of people in this room, the joint duty program in the IC, while not mature like the Goldwater- Nichols was really something that paid huge dividends for exactly the reasons you were talking about: the experience that was gained whether it was in another agency or at the ODNI it was just tremendous and really well conceived. Okay, so we have some time so we're going to switch gear here, switch from my handwritten notes that we're all trained to do in the IC and now I've gone to an iPad. Now it's time for questions from the audience—they're coming in like a stock ticker, so I apologize in advance, we're not able to get to all of them, but let's get to a few. Here's one: "What's the status of the cyber deterrence options developed as part of the President's executive order on cybersecurity?"

TB: If there's a congressman in the room, I know some of you are interested in seeing the reports that were called for in that executive order and we will make sure that within the bounds of appropriateness that we do share them with you and your teams. Here's the status administratively and then I'll give you the status conceptually.

The status administratively, you can go back and look at the President's executive order as being broken into three categories: a category of increasing our defenses to our federal network or networks, and then secondly to increase the defensive ability to protect our critical infrastructure, in particular our section 9 entities- those that are the most critical of the critical infrastructure sector operators. And then thirdly, this section that I'll call two sides of a coin; it's been referred to as deterrence but remember we first have to decide what it is that we think is and is not acceptable and what we can live by in terms of a golden rule and then we can think through what it is that we'll do to those that violate those rules. And so, the status administratively is there are a series of reports called for and recommendations called for in that executive order, somewhere at 90 days that passed now a month or so ago, a month and a half ago, somewhere at 180 days and farther out and so they're not yet upon us. Those reports that were called upon have been provided, only one of them to date I am proud to tell you was late, it was not late by much. I won't name the agency, but I think they were big enough to have a good excuse and you can surmise.

So now what we'll do with that: we'll think through the data that we collected, some of this is extensive. What I didn't want to do was have a confirmation bias problem coming into the office. I probably could've sat down and written what Tom Bossert wanted our nation's cybersecurity strategy to look like and then jammed it past our Congress in a hurry or at least by our Cabinet. I don't think that would've been a wise way to make policy. I'm sure I'd have made a mistake. Instead, what the president chose to do was make sure we validated all our assumptions, make sure we get information and input from you men and women and also from his incoming cabinet. We're getting that information and I think what we'll do on the deterrent side is end up figuring out a means and a method to apply elements of national power outside of cyber to punish bad behavior and we'll try to do it in a way that's commensurate with the offense and also revocable in a way that's not going to create a long-term escalatory posture.

If we have a bad actor that does something increasingly unacceptable, I think what we'll have to do is punish them in a way that's real world and not cyber world. In fact, there's very little reason to believe that an offensive cyberattack is going to have any deterrent effect on a cyber adversary. In fact it's going to encourage them to hurry up and become better hackers, and develop better defenses. I think it's not only a misnomer, but it's something we have to move past and say out loud. At this point we're going to have

to punish them in a way that changes or modifies their behavior while also defending against what will continue to happen regardless of what we do to punish people. You see how difficult a problem it is to apply pressure to the Venezuelan dictator or the North Korean regime, so what we'll do is both.

RM: Terrific. Tough topic for sure. Here's a good question that touches on some of the issues we mentioned earlier and it cuts across many different lines. They're referring to the cyber mission force as part of cyber command and the question is: "Can you describe the process or the concept of how to utilize the cyber mission force to react to a cyber attack on privately owned critical infrastructure? Can you expand and give examples of possible triggers to that action?"

TB: Yeah, so, the first won't be a trigger. The first potential outcome of our public debate that we're about to embark upon would be to allow some of the most critical of critical operators to be within kind of the envelope, as you say, in the British or Israeli model. Let's pick on the Israelis for a little bit because they've provided a lot of good, positive lessons for us to learn from. They'll have the size and benefit of a smaller country but they also have a different kind of trust in their security functions as a government.

They provided, essentially, what I'll call a virtual Iron Dome over their country, and they'll defend everything within it, from a government perspective. It doesn't require a trigger, in their model. In their model, any bad incoming signature is something that is subject to their immediate blocking, mirroring, or rejection, notification or otherwise to the intended target. So it's not so much a trigger as it is their model has allowed them to use their capabilities and their government authorities to protect everyone within their country. We could pursue something that narrowly allows us to do that only to the most critical of users of our Internet and our dot-com, within a carefully constructed set of bounds so as to not allow for any abuse and privacy concerns.

Or, we could do that plus a trigger-based system. A trigger-based system though is what we have right now, I would argue: if we're going to keep it, we're going to have to increase our capacity tenfold. We don't have what it takes right now to see an incoming bad malicious piece of code and then get an FBI agent out fast enough to every potential target. Some of these phishing attacks might end up affecting 20,000 computers, to then take an FBI agent, send them out, and have them knock on the door and say "excuse me your computer might be the victim of a phishing attack and I can't tell you how I know but please take the following remedial steps" would require a significant increased investment in our FBI—which is important but not quite to that level; I don't think that's achievable—but also in our intelligence community. To the trigger question, let's see if we can reframe the question and think through how much trust we can allow our government to have of its people and how much authority we can then wrap around those things that we consider critical.

RM: Terrific. I think we have time for about one more question, so let's --

TB: Let's do two more.

RM: Two more, OK, very good. Here's one with respect to homeland security and the IC. DHS has two IC components—the headquarters intelligence and analysis staff and the U.S. Coast Guard—but other DHS components such as CBP and TSA also gather intelligence and DHS shares the intelligence with state and local officials. What must be done to improve the collection, analysis, integration, sharing in the homeland security intelligence enterprise?"

TB: Yeah, this is my opportunity to say a third time, thank you for that question, that we need to mission integrate by function. I think if you were to go through out DHS right now and ask each individual subcomponent what they're doing to collect information, who sets their information collection requirements, who establishes their analytic standards, and with whom do they share that information analyzer raw you'll get a different answer, a different priority, and a different set of standards in each instance. It doesn't mean, again, that they're doing the job poorly, it just means that we have an opportunity here to improve and my challenge would to figure out a way—David Glawe is going to have his hands full on this—to better integrate, better prioritize across the subcomponents of DHS. It's a large department, 3000-plus people and they have a lot of responsibilities from immigration enforcement to intercostal fisheries enforcement and intelligence can lead into each one of those efforts but it can't be diffuse to the point where there's no prioritization. Right now, what you'll see is an opportunity, I guess I

would call it, to improve that integration and it's going to require some people to let down their guard and allow for some centralized management. I think that there's an opportunity here under Elaine Duke right now to do that and she's got my top cover and support every day.

RM: Terrific. That's a great segue into the last question then, and it comes from one of the universities that are represented here and the question's twofold: one is what's the federal government doing to coordinate or support educational programs for cyber professionals in both the civilian and military sectors? And No. 2, what's the administration's vision for supporting cyber education certifications for career changes of displaced workers or shrinking industries? I guess leveraging industries that may be declining, to retrain them to be more productive for the national security.

TB: Yeah, boy, I'm wide open to ideas on that that are successful. We've had a lot of opportunities to try. Maybe the best way to frame it is to explain to the audience that there are, I think, believable estimates, that there's upwards of 700,000 cybersecurity jobs unfilled. In other words, there's an employer, right now, sitting there thinking "Boy, I really wish I had x… a network engineer or just somebody that's certified enough to manage my IT system and manage it for the purpose of securing my data, and I can't find that person." In a world in which the unemployment rate is still a problem, that is troubling and it is obvious evidence that people don't have the background, training, and experience to qualify for that job; otherwise they'd move and take that job. I don't think it's an indictment of capitalism; in fact, the job rate now that's not filled is also accompanied by some of the highest salaries, so these are unfilled, high-paying jobs.

All the conditions are there to achieve the right outcome, except it takes a little bit of time to cultivate and train people, so I'm wide open to ideas. We've got four or five different initiatives that are being discussed right now—programs that would help train people, programs that would help give them internships and opportunities to them learn on the job. All these things are wide open to us right now and we're willing to try them, and I think the government is willing to invest a little bit in them as well. I wish I had a better answer but we have to find a better way to do it and I think part of what I can do is educating the public, and you can educate the public into knowing this is a viable job opportunity. Encourage your schools to not think of vocational training as a negative thing. I can't believe that "VoTech" has become a bad word, the idea now is that you don't have to go and just learn how to rebuild an engine, which is also valuable, you can go and learn how to secure a network. It's a skill, it's a trade, and it's a high-paying trade when you get out of the educational system. Please take it seriously, please help me with that, and that's the answer.

RM: Okay, great. Tom you've been very generous with your time. I think we're right on time now to get you to your next appointment for the day. Thank you very much, I know I speak on behalf of AFCEA, and INSA, and the audience—incredibly thoughtful remarks, comprehensive, insightful, and we've all learned something today and we're glad that you're in the job so thank you very much.

TB: Thank you very much.