INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Transcript of keynote address by

Bill Evanina, National Counterintelligence Executive

at

Unprecedented Counterintelligence Threats:

Protecting People, Information, and Assets in the 21st Century

Monday, April 10, 2017

9:15 a.m.

NRECA Building

Arlington, VA

Transcript prepared by INSA staff, Wednesday, April 12, 2017

The following transcript has been edited for brevity and clarity.

Transcript – Bill Evanina at INSA, 10 April 2017

Mr. Evanina:

Good morning. So this is my opportunity, I have a few minutes to spend with you today, a very fortunate few minutes, and I'm very humbled to be here. Mr. [Charles] Allen, thanks to you and INSA for having me be available here today and speak to, I think, not only to a robust crowd but the leaders, not only from a thought perspective but people who actually do the counterintelligence and security business, not only in the government but more importantly I think in the private sector. So to be here with you today is a great opportunity for the Intelligence Community, for the counterintelligence cadre of the United States of America as well as the security cadre of the United States of America, because at the end of the day, as you all know, the government doesn't make anything. We spend a lot money buying things, but it's made in the private sector.

And if we're not going to, I would say, not necessarily win this battle, of countering the intelligence mindset of our adversary, but if we're even going to break even, it has to be a team sport. It has to be a partnership. For years and decades the government has used this public-private partnership, the three P's – it's been around for 40 years but it's been a lot of talk. It's been a lot of policies, and a lot of strategy. But I believe because of the threats we face right now from our adversaries – they're not new, they're in the news now, though – supply chain threat, the insider threat, the critical infrastructure threat. None of that is new, but it's in everybody's vernacular now, so we're going to talk a little bit about that and if you look at the construct of what we face every day – team sport, team – which means industry, large companies, defense industrial base, small companies, the mom-and-pop shops. Understanding that the only way we win this – and I'm actually going to include the media in this as well – the only way we win this or break even with our adversaries is a team approach – a whole of government approach plus a whole of country approach. We need to get back to patriotism, we need to get back to the understanding that as the United States of America, I believe the best republic and democratic government ever created – we're at a threshold right now. We have to make a decision where we go. We have to make a decision, do we want to move forward at the pace we're going, you want to understand and to clearly articulate the threats that we see and face every day and deal with them, or do we want to shrug it off and make it a governmental issue. So my challenge to you today as I go through my talking points is think about what you could do to help the process. What you could do to help INSA, what you could do to help other organizations in the public private domain, to create vibrant, effective, and efficient solutions to not only supply chain threats, how we're going to protect critical infrastructure and most importantly, my number one priority, the insider threat.

We don't have to go far down reading the paper to find out what those threats are. But my concern is there's so much of it, a lot of it gets lost in the noise. Some of it gets lost on page 15; some of it doesn't get addressed in the newspaper, doesn't get addressed on cable television. But from what I see, in my position, the threats are real and our adversaries are more brazen now than ever. I could sit here and tell you, whoa, our adversaries have never really addressed supply chain penetration of the United States of America; they have never really done critical infrastructure probing of our SCADA systems. That would not be true, but now they're just a little bit less afraid to get caught. And the private companies who deal with this, who see the malware initiated in their companies, they see the spear phishing attempts on the oil and gas pipelines and electrical grid, the financial sector, they feel that pain every day. And at the end of the day it comes down to risk.

For government, the risk is very clear. We have insider threats that provide significantly damaging classified information to not only our adversaries but to institutions such as WikiLeaks, ShadowBrokers and a lot of other folks. Why do they do that? What truly is the factor that, when that employee wakes up in the morning and decides, I am going to download a lot of information and I'm going to send it to Wikileaks, or I'm going to I'm going to download a lot of information today and send it to ShadowBrokers, or I'm going to send it to the Russians

or the Chinese. I'm that mad. Or, the other side of the coin, I'm so unhappy today I'm going to wake up and I'm going take a gun into work and I'm going to shoot my boss, my coworkers, and then maybe myself.
If you look on the spectrum left to right, whether it's a kinetic threat like the Navy Yard, or Mr. [Nidal] Hasan at Fort Hood, or you can go back to Snowden – whether it's a thumb drive or weapon, they're still insider threats. We have in the government, in the private sector, a collective group of individuals who provide some of the best monitoring of systems and users that we currently have in the marketplace right now. The monitoring of our systems, our people, our data, hasn't stopped the bleeding, hasn't stopped the insider threat.
You look at today's agenda, the first panel that comes after me: the mind of the insider. That is what I believe to be the critical component of stopping if we can, although I believe we'll never stop the individual who wants to be nefarious and conduct insider, malicious behavior; it's almost impossible. Because we are never going to get, in the Intelligence Community, in the government, or in the private sector, to a draconian environment where we search everybody on the way in and the way out. It's just not going to happen. It's not conducive to a workplace that we all want to work in.

But how do we get to left of event? You could have the best monitoring in the world. But if you don't understand the psychology of the individual and the people that work for you to get to left of event, how do you identify that individual prior to making that decision early in the morning to be an insider threat? We have to find a way to do that. We have to find a way to understand Bob or Sue and provide them the venue to act out. That venue could be simple as an employee assistance program. It could be as simple as an interview with someone from the security department; it could be as simple as a peer consultation. But how do we identify that individual?

When we think about insider threat, you can go back decades to the postal service, right? A long time ago. But let's look at what's happened from a linear progression since Manning and Snowden. Now, we put in a lot of time, money and effort into monitoring our systems, our people and our data. Let's fast forward just the last eight months. Have we seen some significant insider threat activity in the last eight months? You just saw last week, the criminal charge of a State Department employee as an insider. Before that you saw the significant breach at the CIA; I'm not going to speculate that investigation continues. Before that, you saw Mr. Hal Martin at NSA. Significant damage, all three, as insiders. But let's look back, back to August. Does anybody remember what happened with the FBI employee in New York. Raise your hand if you remember that. Four – four people. My own agency arrested one of its own for being an agent of a foreign power, for the country of China, in New York City. I think it was on page 11 or 12. Ten years ago that would have been front page news, on every newspaper in the country, and it would have been on every media outlet, cable news and the national news. An FBI employee charged for being an agent of a foreign power, to the government of China – very little fanfare. Significant damage to the FBI, I would say so. So I would ask you if you want to talk about what Mr. [Kirk] Poulsen talked about, State Department employee [Candace Claiborne], Mr. Joey Chun from the FBI – are they contractors? No. So we need to quickly, and I will say urgency, eliminate this mindset that the only insider threats are contractors. It's not true. We have no empirical evidence, no data to show, two things: that the majority or the propensity for insider threat is a contractor and we have no empirical evidence or information to tell us that it's a millennial. A lot of folks in the media want to say, oh the millennial groups, they're more willing and they want to be leakers, insiders. We have no evidence of that to be true. Just look no further than last week at the State Department.

So, if you look at today's agenda, and you put it in totality, it's basically a day in the life of my organization at NCSC. I'm going to talk to you real quickly about what our priorities are; the priorities I have addressed down at the White House and with the partnerships we have in the Senate and the House. Because I am proud to tell you that, currently, we could not have a better partnership in the Intelligence Community than we have right now with Congress. They want to do what's right and they want to do it now. So we collectively have to find solutions and let

our congressional folks help us find solutions, whether that is from a supply chain ideology, how we best protect critical infrastructure or how do we facilitate enhancements and whatever we're going to do with insider threat. And then how do we protect PII, personally identifiable information. What does that mean? Currently, the numbers are just over half of American adults have been victimized by PII theft. And that's just from one country. Half of Americans, which means half of this room. You have a panel this afternoon on OPM, the long-term damage from the breach that occurred, 21.5 million people victimized by the breach at OPM. So, fortunately for my office, we have successfully created a memorandum of understanding with OPM. We have a congressional mandate to a damage assessment on the that data, which we are currently under way collecting information from OPM. We have to condition it, we have to transfer it, we have to drive analytics across it, and then try to figure out what our adversaries do with that data, and how would they best manifest targeting of our employees and contractors that are victimized. Not only the folks who were victimized, but their family members who were in that data: their children, their spouses, their cousins, their co-workers. Our adversaries won't stop to target us; they will go to those depths. So we have to be able to facilitate what that damage is, what it looks like now, and what it looks like five years from now, and be able to put ourselves in the best position to drive understanding, consultation, and threat warning to those we believe are most susceptible.

So our priorities, No. 1, the insider threat. You have a panel right after this, on the mind of the insider. I'm not going to get into their business; but they're the experts on this and I clearly believe you could take all the monitoring you want in the world, it's not going to solve the mental make-up. So you look at the three categories I believe, our Five Eyes partners believe, the FBI's clearly said, that are key to understanding, identifying the insider threat. Number one, narcissism. Number two, Machiavellianism, call it what you want, the ability and want to manipulate others. And three, it's basically a psychopathy, a callous, cold personality. Those three things. I joke a lot about my office and the folks in the security and intelligence community and the private sector, that's half of everybody, right? It really is. But if we understand that and if we could identify, and please understand what I'm trying to say here, if we can at least understand that all the monitoring in the world will not identify narcissism. You could track somebody's keyboard, you could monitor the movement of data, that will not identify narcissism. That will not identify that individual who's been passed over for promotion two or three times in the last 18 months. That will not identify the individual who is going through a very vigorous divorce, who's having financial difficulties, maybe has a child with special needs – is angry at the world, has other issues in the world. There's no auditing or monitoring that could identify that. So how do we marry those two together? How do we understand the individual's mindset and then have robust monitoring on their systems and data? That is the key to success, identifying the insider threat. So number one, insider threat, priority.

Number two, critical infrastructure. I get to see the data that comes in everyday about our adversaries, how they try to and are successfully penetrating our critical infrastructure. When I say that, our priorities are in three sectors, specifically: the financial sector, the energy sector, and the telecommunications sector. There are a lot of critical sectors, do not get me wrong, but we can't do it all. So what does that mean, what are we doing? So DHS and Treasury, do a really great job of facilitating those sector touchpoints for the individuals in that. We add a little bit of the who and the why. So if you have Russian malware or you have a spear phishing attempt from China, or the Iranians are doing something nefarious in our gas, water, electric grid – who is it and why? What intelligence service specifically has done it, and why are they doing it? What's the strategic plan? We could feed that into DHS, into Treasury, provide a little bit better picture to the sector heads and most importantly to the regulators who are out there, whether they be the FCC, the FERC or any other regulator who can deal with the companies who are a real victim of this.

BlackEnergy [malware]. What does that mean? Are we taking a really good look as the private sector and the energy folks who are out there; are they working hard enough to understand what's going on in Europe right now?

What's going on Ukraine? What the Russians are doing in Europe on BlackEnergy? And if we aren't and we aren't understanding how that can manifest here and what we have already seen, what does it look like a year from now? Then we are not making the right risk-based decisions for our country.

The financial sector, I believe we are the best in the world at what we do. Moving money, transferring money, brokering money, investing money, and the little things like our ability to go to an ATM today and take out $20 to pay Chuck for lunch. Right? How does that happen? What can our adversaries do? What do they want to do? And what have we seen them do to identify the algorithms of how that works? The fiduciary relationships that exist between banks and contractors who monitor, make, and maintain our ATM machines – critical infrastructure. Just think about the ifs. Remember what happened with Greece two years ago when the ATMs went down and the money stopped? I think Greece said, hey, 38 dollars per person per week out of the ATM machine. Just imagine if our ATM machines went down. You think there would a be a little chaos here? I think so.

So, No. 1, insider threat, No. 2 critical infrastructure, No. 3 supply chain. Again not a brand new event, but what is supply chain? My frustration has been supply chain and in my few years here, supply chain is like uh the enigma of cyber, right? So we spent two years trying to convince people that cyber is not a country, right? It is not floating in the Atlantic, right? It's not a threat from a nation state; it's a vector. It's something that our adversaries use every day to penetrate us. Supply chain is in the same boat with respect to understanding what does that mean, right? So what we decided was that we would take a real hard look at what we could do to manifest change in understanding the supply chain threat.

When we think about supply chain, you know DOD and everyone here in the defense industrial base they make things. Our acquisitions and procurement folks have forever been trained to facilitate and procure, acquire, under cost and under the time allotment, right? So you can call it what you want on time, under budget. You heard Mr. Allen talk about "delivering uncompromised". What does that mean? To me, that means as we deal with weapons systems, weapons platforms, satellites, the new frontier, and we put rocketry into space and we put our collection satellites; are they going to work? In two years when we are in some type of crazy battle in space, are our satellites going to work? And if they are not going to work, it's because three years ago our adversaries were able to penetrate our supply chain and render something inoperable. So when we're concentrating our supply chain threat mitigation now, it's for things that are going to be useable five years from now. My concern is what we did not do five years ago.

The solution here is, and we will talk a little bit more about our marketing campaign on this, is to aggressively – aggressively – and expeditiously have our acquisition and procurement folks in our security apparatus immediately. Security of what we do – whether you are Lockheed, Boeing, Raytheon; it makes no difference – if you do not have your acquisition or procurement cadre part of your enterprise-wide solution, you are doomed to failure. Doomed; it is guaranteed. You could have the best cyber protection, the best security apparatus; you can be like Lockheed and have a counterintelligence operation with Doug Thomas but if your acquisition and procurement folks are not part of this, everything else is a waste.

Because we know what our adversaries do to infiltrate us in the government, in the private sector – it's through the supply chain and specifically through acquisition and procurement. What we also know is that probably the least-trained employees, whether in the private sector or in the government, are the acquisition and procurement folks specifically in respect to the threat that we face, how the threat is manifested and the basic due diligence that's required to procure contract. We spend hundreds of millions of dollars procuring a contract on company X, but you allow 15 subcontractors and subs of those subcontractors. What do we know about those folks? Raise

your hand if you have ever heard of Nutcracker? Go home and Google "Nutcracker." Go home and Google supply chain threat successes by our adversaries.

Who's heard of ZTE? Five people, six people, maybe eight people? Okay, ZTE you know what country they are from? China. You know what happened last week with ZTE? Anybody? No one? Outstanding, proves my point. I don't even think it made the paper. It didn't make the news, didn't see it in the Post, didn't see it in Times, didn't see it in Wall Street Journal, didn't see it on CNN. So ZTE was a criminal investigation by the Intelligence Community and the FBI started in 2012. Supply chain penetration, I'd say, in government and private sector as well as violating sanctions and embargoes to North Korea and Iran. They just plead guilty last week and agreed to a $1 billion fine. $1 billion, the largest fine ever pled to by the Commerce Department. Think about that. $1 billion and I think three people heard of it here. So what were they doing? What was ZTE doing? They were coming to the United States, they were illegally procuring microprocessors, repackaging them and sending them North Korea and Iran. Not sending them selling them, right? 280-plus known transactions from ZTE to North Korea alone. Is that a counterintelligence threat? I'm not sure how anyone thinks it's other than that, right? Any time you can take restricted electronics or any other kind of parts and send them to the folks that should not have them they are bound to be used against us, right? Again, if we are going to solve these problems it needs to be a whole of country approach.

Raise your hand if you have heard of BlackEnergy? Eight, twelve people. Right? Another significant threat. Raise your hand if you heard the story of the Android issue a couple months ago with 700 million victims of their PII theft being stolen and sent to China? Raise your hand if you are aware of that? Is that a counterintelligence threat? Is that a security threat? Yes it is. It's part of the narrative we have to continue in this group to build. To build that narrative, to understand that the threat we face not only is I would say asymmetric, it's not just following around the intelligence officers in this country, which in my opinion are way too many to begin with. It's the asymmetric side of it.

So again, back to my premise of insider threat, critical infrastructure, supply chain, and the last, which is the old doozy, economic espionage. To me they're all tied together. You look at the best economic espionage cases that have been successfully borne against our private sector, you're going to find an insider threat. You're going to find supply chain vulnerability or success on their part and you're going to find supply chain issue. You want to really get *agita* – it's an Italian word for you people who don't know. You want to get upset and not feel good, go back and just go on to the DOJ website and search economic espionage convictions, just the folks that have been convicted and look at the linear span of just stuff, just from the country of China has stolen from us, from weapons systems, delivery systems, satellite based systems, algorithms from the financial sector, Kevlar, hybrid automotive technology, grain and seed – they were caught digging up in a farm – windmill technology**.** Every type of technology: microprocessors, nanotechnology, semiconductors – you name it. It's depressing. And what does that result from our private sector? Significant financial loss. Not only from the research and development that it has cost years to procure and make. Jobs, because now we don't have the corner of the global market on that particular capability, it's lost so we then have to lay off all these folks. It's a significant issue and my argument is that we have to understand that as a counterintelligence issue, as an active attempt by our adversaries to cause us harm. And if you have pail all these things together and I look at it as one big bucket that we as a group here have to treat as a team sport. We can't win as an Intelligence Community, we can't win as a security entity, we can't win as a counterintelligence entity, and we can't win as a government. There has to be for the first time a true public-private partnership. The private industry, whom I believe is mostly the victims here. We talk about economic espionage is anybody stealing money out of OPM or the FBI or CIA? No. The risk is in the private sector. They make everything. They have the human capital, the investments. There's so many things I'd like to talk about but they're

not set for this environment in terms of the classifications. But the theft and the bleed that we feel every day is pervasive and it's aggressive, and my concern is if we don't find the solution from a protective standpoint and then partner that with a policy aspect of deterrence. We used to say a death of a 1,000 cuts. We're way into 800s right now, 900s. We're getting close to a 1,000. But we're drowned by the noise. The noise is just too loud to concentrate on anything. Which is why, getting back to the premise of why we're here today, and the agenda, which is I believe excellent to understand the nuances of the threat.

You have the leaders in this group, in this room, whether be from psychology, the data, the insider threat, the best practices, and how we're going to look at OPM; it's all right here. I'm excited about hearing this entire agenda, I'm going to be here for the most part of the day because I'm sure I can learn from what we're going to hear about today. But my message is, we have to have a whole of country approach. And how does that whole of country approach manifest itself? In understanding. I don't want to get too far into this because I'm looking at my time but think about what's happened since the election. Think about the word "Russia" and how often we have seen that in the newspaper, on TV, our children come home from school asking about Russia. I know my 12-year-old does. What's up with this guy Putin, he says to me, right? I'm not sure what to tell him. So regardless of the events, regardless of the investigations, regardless of what transpires in the next six months to a year, ask yourself, when Mr. Putin wakes up every morning, is he smiling? Sure is. What I can tell you, and I'm going to be a little bit, I guess, honest here, we'll call it. So part of my job, which I think I have an amazing opportunity to be in this job, is heading up the CI portion of NATO. So for the last couple years, I've had the opportunity to go over and spend time in NATO and listen to our counterparts in the member nations and the risk, and the threat that they feel from the Russians, whether it be Lithuania, Estonia, Latvia, Poland. I have to be honest, a few years ago, I didn't give it much thought. The propaganda, propaganda, propaganda, propaganda. I went over there two months ago, let's just say I am now listening with eyes wide open. Because for a long time here in the US, we were worried about known and suspecte, intelligence officers. We were worried about the specific and clearly opened-faced threat that we face, espionage, the ability of Russians to maybe get someone to commit treason. Clearly the asymmetric threat has changed and always had been there but now, the ability to manipulate us as a country – we have to understand it. We have to understand what it means and we have to be able to work together as a country to find a common solution.

So I'll challenge you – what is that solution? The solution is not just governmental. The solution is private sector. The solution is working the private-public responsibility and the solution is also with our media cohorts. The folks who drive the news, who drive understanding of what's happening every single day. This has to be an American solution. If anything, an American understanding of what's happening to us. I will challenge you in the last few seconds here, to ask what happens next. Because I can promise you, what's going to happen next are more breaches, more data being lost, more insider threats, more successes by entities like WikiLeaks and Shadow Brokers. All that's going to happen and the only thing to stop it, is us. On the one hand, understanding is promulgate the education, the awareness of where we're going with it. I used to say six months ago, even a year ago, subsequent to the OPM data breach, the big solution was controlling the controllables. If you heard me say before, we have as Americans an innate inability to not click a link. We just cannot stop clicking links. Because we can't stop clicking links, our adversaries will never stop sending us spear phishing. And will be successful forever. The intelligence, I see, every single day on the classified side, data being lost by cleared defense contractors, every day, not because of sophisticated techniques used by our adversaries but because someone clicked on a link and allowed malware into the system and they took over as the systems user or privileged user and stuff was exfiltrated. I used to say we have to stop clicking links. Over 90 percent of all PII theft is subsequent to a successful spear phishing breach, but I no longer say that anymore because I believe we have to have a technical solution. From a cultural prospective, I watch myself, I study myself and my inability to not click a link, I study my children,

my one kid, I study the people at work. We have pen testing in the government, I know the private sector has it and we fail all the time. So I believe, maybe we're past a cultural ideal that we can stop clicking the link and we have to have some kind of technical solution. Until we solve this issue of our adversaries' really quick and easy ability to get into our system because we click a link – until we solve that, they're not going to get very sophisticated. I promised the folks who allowed me to come here to spend some time and answer some questions, which I will before I close out. So, have any questions? Anybody? Otherwise, I'm going to close and sit down.

> *Audience Member: Do you have any examples of best practices of private industry companies that have paired really well setting up or improving their defense programs with the government?*

I do and without being really partisan here, I will say that DHS has done a really good job, especially on the cyber side. I think some of the issue has to be with knowing where to go to get that information but DHS and US-CERT has done a really good job, especially in the energy sector trying to help understand what that threat is and what you could do to protect it. Some of it is just awareness capability: what is the current malware, what are the intrusion sets, what are the ones and zeroes look like, to look out for, and I would say DHS and Treasury have done a really good job in the financial sector. But those sectors all have groups to facilitate that data information. Some of it is just awareness of that, but without calling somebody out and getting yelled at later, I'll talk offline.

> *Audience Member: Do you have any recommendations for how Intelligence Community agenices in particular can strike a balance between advertising their CI successes so that people know the country as a whole can get behind what has been achieved but then also still maintain the secrecy to the threat and be able to mitigate the threat?*

Wow, that's a challenge. The CI successes – you're not going to see them in the newspaper, that's for sure. I can tell you from my perspective in the Intelligence Community, I would want to know who needs to know those first, because I believe in the Intelligence Community we see those successes every day and we go home happy and proud of the successes we get to see. Whether or not the public needs to see those is a good question. It's probably worth looking at how do we drive those successes in a mundane way, maybe in a non-classified way, to show that we are striking back. Because I will tell you and it's important to know when you go home today, the men and women of the Intelligence Community, which includes hundreds of thousands of contractors, are kicking butt when it comes to our CI offensive capabilities. I don't think we've ever been better than we are right now offensively, and that does a lot to protect us from our adversaries, not only from countering the intelligence threat, but from an ISIL, Al Qaeda aspect as well. Those folks who work in the Intelligence Community are never going to get credit for that and I think that's the way they want it. But I concur we probably need to do a better job of maybe getting the word out about all the great work that is being done because it is never part of the narrative. I think inside [the IC] we're OK. However, I think my dad, who lives in Pennsylvania, who only believes what he sees in the news, I probably need to do a better job of explaining to him the successes that we've had and continue to have. That's not a bad idea.

> *Audience Member: You mention broadly a mix of technological and personal psychological solutions to many of these problems is there any agency or uhh group of people that you think are doing a really good job of mixing that personal and technological solution?*

Yes, I think there are, and again, without risking losing some friendships, I will say there are a lot of agencies in the Intelligence Community who do a pretty good job of that. We're not anywhere near where we need to be with respect to understanding the psychology of the human being. I think in the private sector probably the same, but

there are a couple that are piloting some efforts. But I will be honest here, some of the issues we're talking about when it comes to, and you'll hear it on the next panel, you really have to get the buy-in from your legal counsel. When you look at successes that have occurred around the globe, a lot of them are predicated on an understanding of what the policies are and were is that fine line to privacy. For instance there are a lot of intelligence organizations who do behavioral testing before they hire folks. The question is do we do that once they get hired, do we do that as part of their reinvestigation process – those are questions that we ask all the time and those really have to get buy-in and understanding not only from your employees but your legal community and privacy and civil liberties folks that you work with. Good question.

> *Audience member: Your comment about the narrative got me thinking we know in the narrative the shortness in cyber security experts the country faces what about the psychological side are we facing a similar thing there and should that be part of the narrative to get this perhaps on a better track?*

We have to find creative and new, nimble ways to do two things: recruit folks in the Intelligence Community and the contracting world with clearances, and be nimble about it and flexible and understand how that process works and at the same time preserve what I believe to be one of the greatest privileges in the United States, to own this top-secret clearance. How do we preserve that capability and get the right folks in? Some of that is narrative, understanding that concept, so we look at how we're promulgating and enhancing the number of states in America who have legalized marijuana usage? So that's already catching up with us, right? Individuals can go, I want to apply, but I've been smoking marijuana for four years because it's legal. I know Director Comey has had some conversations about that recently. That's probably something we should think about. When's the last time we did a study on the usage of marijuana and its impact on having a top-secret clearance? That's one aspect of it, I'm not a proponent of it, but those are the types of things, when you look at cyber, and the technical skills we have to have and the millennial generation right now. Same thing with bring your device to work aspects. We hear all these anecdotal stories, I don't want to work in the Intelligence Community because my Samsung phone is glued to my hand. So we have to figure that out.

My time is up. I want to thank you for this opportunity, Mr. Allen, INSA folks, I encourage everyone to enjoy today's panel. Panelists, for the entire day, be active, have some great questions because a lot of the solutions we're going to find together are going to come from this room.

I can tell you on behalf of the men and women of the Intelligence Community, I am proud to be able to be here representing them and one thing you have to understand is we're all proud Americans and patriots. And the only way we find solutions is as a team and a whole of government, whole of country approach. Thanks.