Transcript of INSA Leadership Dinner Program with FBI Director Jim Comey

Hilton Mark Center, Alexandria, VA
Wednesday, March 29, 2017

Participants

- **Jim Comey**, Director, Federal Bureau of Investigation

Thank you. Thank you for that kind introduction. I did take a shot at the New England Patriots on live television, which I heard about from one of my brothers who betrayed the family when he moved to Massachusetts and became a Patriots fan.

(APPLAUSE)

What I want to do very briefly is share with you some thoughts that are top of mind today for the FBI. And then I want to shut up and take questions that I will try to avoid answering from the great Mike Leiter.

(LAUGHTER)

And I'm determined not to make news, for those of you who are following this...

(LAUGHTER)

First things that are top of mind, I want us to talk very, very briefly about how the FBI is thinking about our cyber strategy.

Can you hear me okay?

(I want to talk about) how the FBI is thinking about our cyber strategy, then I want to talk about a unique challenge to all of our work in the form of ubiquitous, strong encryption, and explain to you why that matters so much to the FBI, and why we are determined to continue to talk about it.

But first, our cyber strategy. To state the obvious for this room, all the threats the FBI is responsible for come at us through the Internet -- counterintelligence, all the criminal threats we're responsible for and terrorists in the following way: to proselytize, to communicate, to inspire, to direct, not yet to use the cyber vector as a way of doing actual harm – inflicting harm on infrastructure – but logic tells us that's inevitable for the terrorists' mind to find that vector. And so, all the threats the FBI is responsible will come at us in that way.

The first part of our strategy is humility. We are standing in the middle of the greatest transformation, I think, in human history. The way we learn, the way we work, the way we love, the way we connect, the way we believe; all is effected by the digital era, the digital revolution.

And so, we stand there with an attitude of humility because it would be foolish to say, we know how the FBI should grow and change and adapt, to me, the transformation that has never happened in human history. We don't know for sure.

We're trying to do things that are thoughtful, that make good sense to us and then get feedback from our own people, from our partners, from our colleagues around the world about whether it's making sense, and then we will iterate.

But our strategy has five parts and actually, two parts of it I want to spend some time on. So, I'll run through it relatively quickly. Our first part of our strategy is we want to focus ourselves and there are two aspects that I want to highlight for you the way in which we're trying to focus.

The first is, the way we assign the work in the FBI. Traditionally in the FBI, the physical manifestation of an event is what drives the work assigning. So, if the bank robbery in Chicago, the Chicago field office works the bank robbery. If the fraud is based in Seattle, the Seattle office.

We've come to the conclusion that the physical manifestation of a cyber intrusion especially isn't all that meaningful, because it's being committed likely by somebody far away from the physical manifestation, it's being committed at the speed of light, and it may be quite random as to where the intrusion pops first.

And so, we're approaching our work in a very different way for the FBI. We now assign computer intrusion work, whether that's a nation state, whether it involves a criminal syndicate, whether it involves a criminal syndicate working for a nation-state, whether it involves hacktivists or somebody else, sort of the motley crew of people who are engaged in intrusions. We assign it based on talent.

We make a judgment as to which field office has shown the best chops against a particular dimension of a threat posed to us by a nation-state and we assign it there because they've demonstrated the ability. But because physical manifestations of intrusions are part of the real world and there really is a chief information security officer and there really is a CSO and a CEO of a company that's been victimized.

We're not blind to physical manifestation, and so we assign the threat to the talent and then we allow up to four other officers to help. The first office is called a "strat" office for strategic. The other officers are called "tact" offices for tactical. And then we have air traffic control from Washington.

This has had a great effect inside the FBI because it has fostered an intense competition among field offices togenerate and demonstrate the talent against various dimensions of the threat. And so, if Little Rock shows they are best against a particular intrusion set from a foreign nation, it goes to Little Rock, regardless of where the hits are from that intrusion set.

So far, it's working pretty well. So far, the air-traffic control has worked well. But again, we stand here with humility and if it isn't working in some way, we're going to iterate. That's the way we're now assigning the work.

The second way we're trying to focus ourselves is on stealing your talent, and here's what I mean by that. The challenge we face at the FBI is that to have a special agent work in cyber, we need a variety of things. We need high integrity, we need fitness, we're going to give you a firearm on behalf of the FBI, you have to

be able to run, fight and shoot. So, we need integrity, fitness, then we need smarts, we need intelligence and then we need specialized knowledge to make you a cyber agent.

That collection of attributes is rare in nature. You may find integrity, somebody who can't do a push-up, who has great specialized knowledge and general intelligence, or we'll find somebody who has great specialized knowledge, can pump out a push-up, but wants to smoke weed on the way to the interview.

(LAUGHTER)

And so, we stare at the pool of talent and we have two reactions to the pool. We can't compete on money. You, in the private sector have more money than we do. We acknowledge that to the people we're trying to recruit. Then we also make sure they understand that life with you is soulless and empty.

(LAUGHTER)

(APPLAUSE)

He said half-kiddingly. And if you want to do work with moral content, come to us. It's not about the living, it's about the life. A pitch that I know worked for a lot of you in this room of ours. And so, we try to recruit on moral content.

And then, we're trying to think differently about how might we generate that talent in a number of different ways. We're considering, do we really need gun carrying special agents making up an entire squad? Now we have squads of eight around the country.

Should we instead have two special agents and six something else's, maybe people of integrity, people of high intelligence, people who have specialized knowledge, we don't give them a gun because they don't have that physical attribute? Maybe.

Something else we're considering is if we can find that integrity, that physicality and basic high intelligence, should we grow our own? Should we build our own university to take that talent and raise it up to be cyber talent? Maybe.

And should we also do something else that'd be very, very new for the FBI? Should we try to make the barrier between us and the private sector semipermeable, so that special agents might come and work for the FBI and then go work in the private sector, and then come back?

The current rule requires anyone who leaves for 24 months to go back through Quantico and that's a painful experience for people in their 40's. They all want to come back because they discover your lives are empty and soulless – (LAUGHTER)

-- and so, they want to come back, but we've made real barriers to their returning. And might we be able to encourage people from the private sector to come work with us as that something else? Don't have to go through Quantico to learn to run, fight and shoot, and then return to the private sector.

Our minds are open to all of these things because we are seeking a talent -- talent in a pool that is increasingly small. So, you're going to see us experiment with a number of different approaches to this. And then I hope when you see us doing something that doesn't make sense, you'll tell us. When you see us

doing something you think we ought to do more of, you'll tell us that as well. And it will be met with an attitude of humility. So, focusing in a better way our work and on how to get our best talent is our first part of our strategy.

The second part is we need to make sure that we -- inside the government -- have our act together in such a way that it doesn't matter to whom a victim of an intrusion or a cryptoware attack or some other attack -- it doesn't matter who they tell in the Federal Government. We're in that place when it comes to counterterrorism.

You walk up to an FBI agent, a Deputy Sheriff, a Police Officer, with a piece of information about a terrorism threat it will get to the right place very, very quickly. It doesn't matter who you tell. We've got to get to that place inside the Federal Government. We made a lot of progress on that, trying to understand the rules of the road, but we still have work to do.

The third thing we're trying to do is impose costs. I don't know of a cyber intrusion that has ever been committed high on crack or inflamed by finding a lover in the arms of another. These are crimes, these are intrusions, these are attacks that are committed with reflection and calmness at a keyboard.

We think that's an opportunity for deterrence, for influencing behavior. And so, we are keen to make sure that attacker, whether it's somebody sitting in a Government office halfway around the world, or in a basement somewhere in the Pacific Northwest, that they feel our breath on the back of their necks, maybe literally, but at least metaphorically, as they begin that intrusion activity.

We think we can shape behavior by locking people up, and where we can't lock people up, by sending message of pretty scary deterrence, faces on wanted posters. And people sometimes say to me, yeah, but the hacker is somewhere halfway around the world working for another government or they're sheltered by a government, how are you ever going to get them?

And my response is, life is long, the world is short, we are dogged people. We just gave up on D.B. Cooper.

(LAUGHTER)

And that took us about 52 years, I think. For those of you who are young, he was a guy who jumped out of an airplane over the Pacific Cascades and we hunted him for 50 years. We're pretty sure he's dead now, so we're giving up. But when you face goes on a wanted poster, we are not going to give up in your lifetime. And that can change behavior. So, you will see us trying to send those messages to shake people as they think about intrusions.

The fourth aspect of our strategy, I won't spend a lot of time on, is to help our brothers and sisters in state and local law enforcement, raise their digital game, because everything they do requires digital literacy. In the good old days, a narcotics detective would roll-up on a location, execute a search warrant at a drug house and find not just drugs and money, but one of those black composition notebooks and the dealers would have written who got how much and how much they were and that had to be photocopied and an exhibit sticker put on it and you were good to go.

Today, there's no black composition notebook. There's a PDA, there's a thumb drive, there's a laptop, there is a digital device. We have to help our colleagues get to that work in a quality way because there's simply no way the FBI could be part of helping with all of it.

I'm told that people get emails from me when I'm in Nigeria asking for money to be wired.

(LAUGHTER)

I usually identify myself as the President of Federal Bureau of Investigation. Don't send me any money, but people do get ripped off and the Bureau can't reach all of that. So, the fourth part of our strategy is help our partners raise their game and there's a lot behind that, but I'll leave it there.

The fifth thing, which is the one I want to spend just a few minutes on, we must get better at sharing information across the boundary -- and there should be a boundary between the public sector and the private sector. We have to find ways consistent with the law and policy and tradition and culture, to make the barrier between us and the private sector semipermeable in some fashion.

And the reason for this is, nearly all of the intrusion activity in the United States -- coming at the United States hits the private sector. All the victims are in the private sector, all the indicators are in the private sector, all the evidence if you want to go criminal, is in the private sector. We are not nearly good enough at getting information from the private sector to us, or getting information from us to the private sector.

This, I believe, is actually a problem not so much of law but of lore. And the biggest problem, I was a General Counsel as you heard, the biggest problem is people like I was -- who are spotting risks and calling them out. Because if we give that information to the Government, will it be used against us in a competition? Will it be disclosed to Congress in some way that it becomes public? Will we get sued? What will our shareholders say? How will this hurt the enterprise? I see too many risks.

What you ought to do is hire one of the great firms that can help us remediate and let's get back on with our business. Even people saying, yes, our files are locked up with ransomware, let's just pay the ransom and get on with it. Most of the intrusions in this country are not reported to law enforcement and that is a very bad place to be.

People are foolish and short-sighted to think that their interest in the private sector are not aligned with ours when it comes to this. Because you're kidding yourself if you don't realize that the hackers will be back, if not to you, then to your subsidiaries and your supply chain. Those with the ransomware will be back, especially if you paid them off. Our interests are aligned.

The challenge we face is having the private sector know us well enough to realize we understand what a victim is and we treat victims for what they are, which is victims. And we do not re-victimize people. Whether that's a sexual assault case or an armed robbery case, a Mafia case or a computer intrusion case -- we have lots of practice at this.

Our challenge is, people don't know us well enough. There is too much confusion and skepticism and distance derived from misunderstanding and myths. So, the FBIs mission is to get out and talk to the private sector and let you know what we're like.

Now, I liken this to a journey, that the CIA and the FBI travelled since the mid-1980s. And that's what I mean by the difference between law and lore. Most of the people in this room know that in the mid-1980s, the Classified Information Procedures Act was passed that offered us certainty about how sources and methods would be treated and protected, if the Government decided to use a criminal prosecution to

incapacitate, to reassure the intelligence community that we're not going to blow sources and methods, there's this framework and here's how it will work.

That did not get the job done because that's law. It took us 20 years of building trust, case by case by case, so the intelligence community came to realize, you know what? This really works, we really can trust the FBI to protect our sources and methods, to use these tools that have been on the books since the 1980s and use them in a way that protects us.

That took us two decades to build that trust. It is in a very healthy place today. It is not in a healthy place when it comes to the private sector.

And so, my ask, those of you who run companies, who are the chief security officers, the general counsels, the CEOs -- if you don't know someone at the FBI office where your facilities are, you're failing. You are pushing on an open door, come and talk to us, understand in the event of an intrusion, in the event of an attack, what is it we need?

And you'll discover we don't need your memos. We don't need your emails. We need indicators of compromise. We need to know how did the bad guys come? What are the signals, what are the indicators that we can use to attribute and to try and pose costs and to help you get over this attack.

The Sony attack was a vicious, hugely damaging attack. It would have been worse if Sony hadn't invested the time to know us before the attack. Every single one of you works in a facility that your local fire department knows the general layout of, right? They don't know your intellectual property, they don't know your secrets, but they know where your standpipes are, where your elevators are, they know the general layout so that in the midst of a smoky disaster, they can save lives.

We knew Sony in that same way. We didn't know their secrets, we don't know their intellectual property. We knew their key people, we knew their facilities, we knew the layout of their network -- generally. And that day, within hours, we were on the ground helping stop the bleeding.

The private sector has to get to know us better if we're going to be more effective. But it doesn't stop there, because it's bad that people don't share information to us. We don't do a good enough job at pushing information to the private sector.

We have a cultural impediment, which is, we have this information. If I give it to them, are they going to jeopardize sources and methods. Sometimes we forget that you don't need the sources and methods. You need indicators of compromise, so you can figure out how they're coming at you.

And all of you in the room know this, oftentimes private sector partners don't realize what ORCON means. Oftentimes, the FBI will have a piece of information. We can't just turn it over to you even with a terror-line. We've got to go back to the people who own that information and gave it to us, but we can do that so much better than we're doing it today. We will get better. I hope you will help us get better as well.

And the last thing I want to leave you before I start avoiding Mike Leiter questions is this.

(LAUGHTER)

I intentionally did not talk a lot last year about the challenge we face from ubiquitous, strong encryption. Our judgment at the FBI was that this is a complicated issue with legal aspects, technical aspects, policy aspects, values -- it was too complicated to discuss during an election year. I know you're thinking you're totally wrong, we could have nailed this during the election year, but we decided that we would not force a conversation about it, but that we would use the time to try to collect data so we could show people what's happening to our world.

And here's what's happening -- if you imagine, the FBI works in a room. A corner of that room has always been dark for the last 20 years. Sophisticated actors could always find encryption to lock-up a device, encryption to cover data in motion, the sophisticated actors, nation states, near nation state actors.

What's happened since the summer of 2013 is, that dark spot has started to spread through the entire room. Ubiquitous default encryption on devices, ubiquitous default strong encryption on apps and other forms of communication has spread the shadows so it's starting to cover more and more of our room.

I'll demonstrate this with the facts of our encounters with devices. October, November, December -- 2,800 -- 2,800 devices were presented to the FBI in the United States with lawful authority to open them. Some from FBI investigations, others from state and local partners. They gave them to the FBI saying, we have a court order, can you help us?

In 43 percent of those cases, we could not open those devices with any technique. That is the shadow falling across our work. And they may say, who cares? I don't know, but I think America needs to have a conversation about this. Because I care deeply about privacy. I treasure it.

I have an Instagram account with nine followers. Nobody is getting in.

(LAUGHTER)

They are all immediate relatives and then one daughter's serious boyfriend. I let him in because they're serious enough.

(LAUGHTER)

I don't want anybody looking at my photos. But I treasure my privacy and security on the Internet. My job, like a lot of people in this room is public safety. Those two values, privacy and safety, are crashing into each other.

But I actually believe something more fundamental is happening. Especially with regards to devices, those devices contain so much of our lives -- our business life, our social life -- our lives are on those devices that we wear on our hip or we carry in our pockets. That's a great thing. That has made us better in lots of different ways.

But it's also introduced with ubiquitous default encryption a concept that's new to America, which is absolute privacy. We have never had absolute privacy in this country. This country was founded on a bargain, which is your stuff is private unless the people of the United States need to see it.

And then with appropriate predication and oversight -- obvious example of that being enshrined in the Fourth Amendment -- the government, the people of the United States can see your stuff. They can go

through your safe-deposit box, your sock drawer, your car. They can actually compel you to say what you remember in appropriate circumstances. We've never had absolute privacy.

The bargain was, we have this privacy that can be invaded with this predication oversight, so we achieve a balance between privacy on the one hand and security on the other. What's happened to us now is we're drifting to a place where absolute privacy is a huge feature of American life. There are wide swathes of American life that are now off-limits to judges. I'm not offering that as a value statement, that's just a fact. That's a different way to live.

If we are going to change the fundamental compact at the heart of this country, it should not be the FBI that does it, it should not be companies that are making amazing devices that do it. The American people ought to do it. And so, what I'm determined to do is not tell you what we ought to do to solve this problem, but to tell you there's a problem and to urge all of you to participate in this conversation.

Maybe at the end of the day we say, you know what? The benefits of privacy in this instance are so important that we'll put up with the tradeoffs. Or maybe we say, you know what? The tradeoffs are so significant, we ought to see if we can't find a way to optimize both of those values better than we are today.

And I actually reject the idea that it's too hard. I actually don't think we've given the shot that it deserves. I don't know anybody in the private sector that's actually making devices who is incentivized to try to figure out how to optimize those two values. They sell privacy, I get that. We're responsible for public safety. Somehow, we have got to bring those two together.

The FBI is an example of how it could be done. We give devices to some of our agents, some are here today. We give them devices that we work very hard to make secure. But, we retain the ability, in appropriate circumstances, to access that content.

It does not require weakening encryption. It does not require giving the Government a backdoor of some sort. I could actually imagine a world where someday, if you're going to sell devices in the United States, you're required to be able to comply with judicial orders. You figure out how.

I don't know whether we're going to go there, but first, we have to have a conversation about it. So, you're going to see the FBI trying to supply data to this conversation, stories of how it impacts our work, so that we can foster and inform debate.

Because what I don't want to have happen is – I have six years and a few months to go – that six years from now people say to me, hey, how come you didn't say something? I'm going to say something. This is effecting our national security work, counterterrorism, counterintelligence and all of our criminal work in profound ways, which you would expect because we're now living in a different way. We should talk about it.

And I thank you so much for joining that conversation and I will look forward to Mike's questions.

Conversation with Michael Leiter

Participants

- **Jim Comey**, Director, Federal Bureau of Investigation
- **Michael Leiter**, moderator

LEITER: And I'm going to jump right in to what I think everyone in this room, and many people watching on C-SPAN probably want to know about. A big question, what do you think of how the FBI has changed the uniform crime reports?

(LAUGHTER)

Is that not why you're here?

(LAUGHTER)

Quite seriously Jim, a lot of people talk about Bob Mueller having one of the most incredible early tenures as director of the FBI, coming in a week before 9/11. You didn't get hit with that tragedy that we all experienced at the beginning of your tenure. But, since July of this year, you have been in the midst of what we now know are two criminal investigations involving broadly the Presidential campaign.

And without asking about that because I know you'd just evade the question anyway, can you reflect just a little bit on your approach to decision making through all of that, especially being the Director of an FBI for two Presidents, carrying over between administrations, as the statute Congress intended the position to be.

But your decision making through all of that and how, as someone who is part of the intelligence community, part of law enforcement, part of the Department of Justice -- has to build that trust with a first customer and simultaneously so deeply involved in incredibly sensitive criminal investigations.

COMEY: That's an easy one, thanks Mike.

(LAUGHTER)

COMEY: First, I think Bob Mueller's early tenure was much harder than mine. I'm not just saying that, I think it was much harder. He came in the week before 3,000 people were murdered in our country. And then he had to not only deal with that, oversee the investigation, but transform the FBI and I inherited a transformed FBI. So my job is a lot easier, honestly.

The last year -- it's been almost a year now -- has been both difficult and easier than you might think. And I'll tell you, I've never been prouder of the FBI. What makes it easier, we're not on anybody's side, ever. We're not considering whose ox will be gored by this action or that action, whose fortunes will be helped by this or that -- we just don't care and we can't care.

We only ask, so what are the facts? What's the law? What's the right thing to do here? And often, we find ourselves choosing between bad and worse, having difficult short menu of options. But in a way, that's

been easy, because that's how the FBI is. So, people I think sometimes look at me and say, look at what you did, look what you did.

Actually, the FBI made these decisions in a high-quality way. Now, the painful part is that we confuse people. And the reason we confuse people is, most people see the world differently than we do, especially in a hyper-partisan environment.

Most people are wearing glasses that filter the world according to side. And this is a challenge I face when I testified in front of Congress, and it's not a criticism of Congress. They see facts as to how it will affect my side. How does that argument effect my side? And when then they encounter people -- and I'm just one of 37,000 that are like this at the FBI -- who never consider side, it's confusing. Like -- OK -- so you're trying to help this person and help that person.

One of my daughters share with me last summer -- maybe late last summer a tweet and I actually I'm on Twitter now, I have to be on Twitter. But she -- she showed it to me and it said, that Comey is such a political hack. I just can't figure out which party he's for.

(LAUGHTER)

COMEY: And I smiled and I took that and I shared that with my senior staff, I said, that is the greatest compliment. We confuse people because a lot of people can't imagine people who aren't considering side. Now we're not fools. I know when I make a hard decision a storm's going to follow, but honestly I don't care. If I have thought about it carefully and am doing the right thing, making the right judgment, it doesn't matter what's going to follow. Because it's not about that, and honestly the death of the independent FBI would lie down in the path to considering impact. If we ever start to think about who will be effected, in what way by our decisions in a political sense, we're done, and so, we never will and in that sense it's easy. The misunderstanding of a lot of people about us can be painful, but the easy part is, we know what our north star is and we're fixed on it.

(APPLAUSE)

LEITER: Follow up a little bit on that, in that, the intelligence community at large and the FBI's part of that, as I think always relied on the select committees on intelligence to provide you the breathing room to do those things in a non-partisan way. And the reasons those were select committees were to make sure that their oversight was more non-partisan, if not perfectly non-partisan in many of the other committees. How much harder does it make your job when partisanship starts to enter into those realms of oversight? Those groups that are supposed to say, no don't worry. Jim Comey can't tell you everything he's doing but trust him. He's doing it right. He's following the law. We're doing the oversight, and you as Americans should feel both safe and your privacy is protected.

COMEY: Yes. That's a great question. I don't want to comment on current events, so maybe I can just talk in general. It's vital that we, the intelligence community, need to be able to share with the American people through their representatives the most important things we're doing, for a bunch of reasons. First, they ought to know and second, there's a danger in all humans and -- and especially when you're an authority in the government. It's captured on something John Adams said to Thomas Jefferson which is, he said, power always thinks it has a great soul. There's danger. I think I'm an honest person and there's a danger, I'm falling in love with my own view of things.

So that checking and that balance is the genius of the design of the founders, and so it's vital that we be able to tell them what we're doing so they can ask hard questions about it. And in my experience, it is a highly productive relationship. Now sometimes, people outside of that world don't understand it. How come you're only telling a select few, because of the nature of the work. There are things we can't let this nation's adversaries know. We have to be able to share them with our oversight committees, and by in large it works very, very well. The challenge in general, in a polarized environment, is that -- again those glasses of side can get in the way of a robust oversight, and make is sometimes difficult for the intelligence agencies. But here's the truth, we find a way. We find a way, because we need each other too much, because we all believe deeply in the design of this country and we find a way to make it work.

LEITER: Right. By the way, I'm just happy when you check back in to government, you've got your soul back.

(CROSSTALK)

COMEY: I left it at a bus station. I got it back.

LEITER: So, I'd like to ask you a little bit about signals intelligence, and not just signals intelligence but really electronic exploitation at large. Because, the one of course might be the device that you find after a raid versus what you're intercepting. And I want to push a little bit, I'm just a middle aged country lawyer, but I want to push you a little bit about that Fourth Amendment analogy that you drew, that we've always had disagreement, this balance between privacy and security needs or law enforcement needs for the government.

It strikes me that at least two things have changed though. One, there's more information out there than ever before. So in 1787, you couldn't figure out what Jim Comey was saying to Mike Whiter for the past five, 10, 20 years. You could maybe just listen to that moment, or just look at his papers and not have everything. Second, in those days of a court or a magistrate approving that search warrant in 1787, that privacy protection that he had didn't cause any problems for anyone else. And one of the criticisms of what went on with the IPhone experience was that by asking for a back door for one, you are not just impinging on that individual's privacy appropriately, but potentially impinging on everyone else who used an IPhone on their privacy. So, how do you think about those and probably other differences from the compact that was struck in the 1787?

COMEY: Yes. That's very fair. And that -- you've pointed to two things that make this a hard debate. One, I didn't think we could have an election year, but to take both of them. There's no doubt that there is more digital dust about all of us out there than ever before, couldn't even imagine 30 years ago, and that we're able to communicate in ways that were unimaginable. I have two reactions to that. One is, the bad guys are able to communicate in ways that were unimaginable 30 years ago. Best example is ISIS' reaching into this country through Twitter, especially in the summer of 2015 to find people willing to kill on their behalf, and then moving them to an encrypted end to end app. That would have been unimaginable when you and I began our careers. And so, there's no doubt the opportunities for law enforcement or the intelligence community to gather information have gone up dramatically, but so have the ability of the bad guys. Second thing, metadata is great, incredibly useful to try and establish patterns of connection, but especially when it comes to the FBI who's business is incapacitating through conviction beyond a reasonable doubt. It does not get you there.

You will not be able to -- maybe in some circumstance I can't imagine, meet that threshold to a jury simply by saying, I see these connections between them without any sense of content, so that's the first piece. What was your second one? I forgot already.

LEITER: Impinging on other people's privacy.

COMEY: Yes. That's the technical --

LEITER: -- And by the way, let me -- sorry -- let me add something to that. When you went to the vendor in the IPhone case, the argument was, well we can keep it safe. But since then, I don't know who, but someone has sued trying to get the name of the vendor. And the Justice Department is saying, we don't want to do that because the vendor might not have the same protection as the FBI does, and hence, we'd be putting at risk what we used if we disclose the name of the vendor. Doesn't that very much go to the argument that any backdoor causes privacy implications for others?

COMEY: Yes. I think it's a reasonable argument to raise that, whatever solution we have should optimize in the best way both security and privacy. And there are clumsy ways you could do it, that would expose all devices to an intrusion, which is why I say this until I'm blue in the face. I am not in favor of government mandated backdoors. If I were asked to imagine the future I laid out for you, what I imagined, is a world where the companies are saying, you want to sell a device in the United States, you figure out how to do it. You figure out the most secure way to do this. And look, again, the problem with this debate is too many people tweeting at each other. It is a complicated conversation, but I don't buy it's too hard.

There are plenty of companies today that are selling devices that are default encrypted and their cloud services are not. I hope they're able to sleep at night. Right? I happen to think they put reasonable security around their cloud, and so when we serve them with a search warrant, they produce what's in the cloud. And so the notion that we're all fatally at risk or exposed, if the government is able to serve judicial process -- I'm just not buying. A lot of work's been done over the last year inside the government, to figure out what could be done to optimize both of those. I'm not going to go into the details right now, but it's not impossible.

LEITER: Would you talk about cyber a lot and some really interesting things you're doing for the workforce and control of investigations outside of an individual field office, or the traditional responsibility. Do you see other changes that need to happen in the U.S. government? We haven't seen the EO, the Executive Order yet on cyber from this administration, but in terms of organization. Although, I think the FBI did amazing work with Sony for example. Sony also dealt with two or three other Federal agencies and there was sometimes confusion and there has been in other cases. Who's in charge? Who's responsible? The capabilities of each of those workforces, how can we do better optimizing all these various pieces of this puzzle?

COMEY: Yes, it's a great question. I think where we are today, the lanes in the road that the Obama administration laid out, which to my mind simply just captured in writing what we'd already developed to, are fairly clear to us and make good sense. The FBI's responsibility is to investigate in response to intrusions, share information that we gather from our investigation. DHS' responsibility, in the main, Secret Service has a role similar to ours, but in the main, is to help with remediation and hygiene and the DNI and the other parts of the intelligence community working through the DNI, are to provide threat indicators. Intelligence about what's going on in the world.

Now there's an interesting question that I'm not expert enough to answer, as to whether there's a role for NSA to play outside of government networks, DOD networks, as part of their security function, defensive security function. I don't know the answer to that. I actually think we're in a pretty good place where everybody understands their role inside the government and I think moving to the place that I said we have to get to where, it doesn't matter who folks call. You call us about something, it looks like it belongs to the Secret Service, we share it. But I think we're in a reasonably good place. Now that doesn't mean that we can't be better, but that's how I'm thinking about it.

LEITER: Getting away from cyber and electronics for a minute. We clearly had a state of leaks over the past, really, five years, going back to Chelsea Manning, moving into Edward Snowden, recent arrests also associated with NSA. A number of those have come from U.S. -- from contractors working for the U.S. government. Do you have a perspective on that? Is that part of the problem? Is there something else that we should be doing to protect this data? Not even touching some of the leaks that have been criticized over the past three to four months.

COMEY: Yes. And I'm not going to talk about anything that's recently reported, for reasons I hope you all understand. We don't ever want any of the business of confirming that something was classified information, by talking about something that was in the media. So I'll go further back.

There's no doubt that there are improvements that we in the USG can make with respect to the way in which we know all the people working on our campuses, both employees and contractors. And Jim Clapper, since Snowden, has been driving improvements in that way. We're not quite where we need to be yet, but there's no doubt that the answer is for all of us to know our people incredibly well. And that if we are relying on periodic re-investigations, relying on the polygraph, all of which may be important tools, we're not doing it well enough. That five years is too long to wait, and these theft cases by insiders remind me a lot of when you see on the news something about a terrible crime in a neighborhood. Somebody always had a bad feeling about the guy, and -- or take our terrorism cases, friends and family almost always saw something. And so we look back at the cases we've had inside the government, including inside the FBI over the last 30 years, there's all kinds of flags that were popped. We have to get better at collecting that data in an appropriate way and popping the flags, we look at the person now not five years from now, and we have to find a way for that to be true for contractors as well as for our own employees. And then the last thing I think we need to work on is making sure we have a uniform security culture. And this is a challenge when you have a lot of contractors on site, because sometimes they don't feel like they work for you, and so they don't need to buy into your culture. Somehow, we together, private sector and public, have to figure out a way to drive a high security culture into everybody no matter what color their badge is.

LEITER: Another issue which has been in the press has been immigration and vetting and the FBI, obviously, does not have a role in determining immigration status and the like. But you have been quoted as to the U.S. government's ability to vet people who are coming into the United States, and strikes me that there's a common misperception that you said, we can't vet any of these people. The FBI does play a role in vetting. What is your view on how effectively we can vet people who are coming into the U.S., of any sort?

COMEY: OK. We, the bureau and our partners, the intelligence committee, have a critical role to play in vetting refugees and others looking to move to our country and we can always improve that, and I'm always looking for opportunities to improve it. We dramatically improved it after 2008 to 2010. We discovered some weaknesses in our system, and so we have gotten our act together in a good way and making sure that if there is any dot, anywhere in our holdings in the U.S. government, we're going to find

that dot and connect it to that person. The challenge, which I've talked to you about before, and I hope people understand what I mean by this is, when someone is coming from a place where there're unlikely to be dots, unlikely to be things that are holdings that connect to them, say from a place like Syria, we can -- have the great systems, talk to each other.

We will not be able to buy down risk in a way we might if they're coming from another place we have a robust relationship with that country, including Iraq. We've got lots of information we've collected in Iraq since 2002-2003. The challenge of people coming from places where we don't have those relationships is, as good as our systems might be, we're not going to have any dots to connect. That was the point I was trying to make. I'm not involved with policy decision about who should come in and how many, that's not our business, and we are working constantly to improve our vetting, but that's what I meant by that.

LEITER: Great. I'm going to start transitioning to some of the many gray questions we got from the crowd. And there were several about recent terrorist attacks, San Bernardino, the Boston Bomber, a discussion of what has co-locally been come to known as lone wolves. Is that a term that we should keep using? Does that mischaracterize who and what they are? And if you could also speak to the challenges you faced after Boston and the changes the bureau has instituted as a lesson learned from that unfortunate event?

COMEY: Yes. I don't like that term at all, because it conveys -- I worry that it conveys to these -- these wing nuts a sense of dignity and I don't want to give them any kind of dignity. They're troubled people who are seeking meaning in a misguided way. It often leads them down a path of killing and harming innocent people, so I really don't use that term. It continues to be a major feature of the FBI's work, because all of human experiences in some ways is a search for meaning and there are troubled people all over the United States who are attracted to the idea of finding meaning to the hyper violence offered by the group of savages that calls itself the Islamic State. And so we have investigations in all 50 states, trying to understand, where are these people, these troubled people?

And I keep saying troubled, but I mean they're people with drug problems, mental health problems, sexual abuse problems, you know, all kinds of issues that lead them in a misguided way to seek meaning and we're trying to evaluate. So where are they on the spectrum from consuming the poison to acting on the poison, and that is really hard. It's a nationwide search for needles in a haystack, but it's actually harder than that. We're just not looking for needles in a haystack, we're looking to try and figure out which pieces of hay might turn into a needle and then it gets harder still, especially with the Islamic State.

If they find a live one, they would move that needle to a place where it disappeared, so it's an invisible, encrypted needle in a nationwide haystack, and it's the reason it's at the center of the FBI's work today. To find them and disrupt them before they kill and on to tell this audience, it is incredibly hard work. We'll always trying to figure out how to do it better, but it’s incredibly hard. One of the ways we've gotten better since the Boston Marathon Bombing is, we are better sharers of information with our state and local partners. Anytime something happens, we stare back at it and say, OK, what could we have done differently or better? We've done that with Orlando. We've done that with San Bernardino.

Every time something happens that involves a terrorist attack, we do that and Boston, one of the things we realized is, we can make clearer that the default is share and we can make clearer to our state and local partners what the inventory was in the Joint Terrorism Task Force. So now, all over the country, we invite the leaders of the agencies that are part of it, on a regular basis, some as often as every two weeks, some once a month, come in, we'll talk about what cases came in and we're closing, what cases are still open and

get your feedback on them, and if you want to follow up on some of them you have that opportunity to do that. We've gotten better as a result of that.

LEITER: Two quick follow up questions then. You talk about that transition from a piece of hay to a needle, which I think is just a beautiful -- well a really terrible, but accurate picture. Do we need a system like some of our European allies have of an ability to engage that person, possibly not with the FBI, not with law enforcement? Some sort of diversion program like we have with low level drug offenders to try to keep them from becoming needles in the first instance and not just wait for them to become needles?

COMEY: All of us in the CT business have our minds open to trying to find ways to do that. We've worked hard over the last four or five years to see if we -- Department of Homeland Security and other partners, could build such a thing, so far with limited success. The challenges, there is no typical person, no typical journey, because the search for meaning is individual. We're talking about people from the age of 15 to the age of 62, all over the country, all different troubles, all different backgrounds and so finding in a repeatable way indicators and then reliably off ramping people is sort of the holy grail of this work. And I haven't found anybody around the world who's doing it in a repeatable, validated way yet.

LEITER: Second is, I want to weave something from your answer here to some of what your previous comments were about cyber and then pull in also counter intelligence. I don't think there's any doubt. We know we're probably in one of the most complicated and heavy flow of counter-terrorism issues that we've had probably since 9/11. The volume and the speed with which they're coming is probably unmatched in the past 15 years.

On the cyber side, you clearly face innumerable threats at this point, and your ability to do all the things you want to do is challenged.

And I think it's also fair to say from the public information, that the counter-intelligence world is not slowing down, and if anything it's probably speeding up. How do you have remotely the capacity to do all of that and at the same time, do all the other pieces that the FBI is so critical to in aiding thestate and local law enforcement for organized crime, white collar, public corruption? And do you have the budget to get that done?

COMEY: Yes, it's hard. It's a good thing that our people never sleep, but here's the truth. The FBI today is about twice the size it was when my friend Louis Freeh was director. We're on a path now to be at full strength by the end of this fiscal year, which means 38,000 people. And, by in large, we have the resources we need. Now there are challenges. Summer of 2015, we were strapped, because we were following people all over the country who were moving towards very dangerous needle territory. And I was asked in Congress, do you have enough resources? And my answer was, if this keeps up I will not, because we were pulling agents and analysts from counter intelligence work, criminal work of all kinds to cover these people. And I guess I should say this, it's only easy to follow people 24 hours a day on TV. It is really hard to do in a clandestine way, and so we were strapped. That wave went away, in part because a number of people, who were with ISIS in Raqqa, Syria were taken off the battlefield by our colleagues in the military.

And so, I think by in large we have the resources. We have to make lawful judgments about what we need to be addressing and what our state and local partners need to be addressing. And the FBI is a pretty complicated process to decide what to do, where we ask each field office to look around your area of responsibility and say, so what are the bad things that could happen here. Across all of the FBI's

responsibilities, who else is working to address those threats, and given the magnitude of the harm and the other efforts already in place, where would we rank that? And we rank without regard to discipline, we rank it across all of our threats and then we do that at a national level and that drives our allocation of resources. So what's going to happen is, if a particular state is doing a great job of adjusting gang violence, state and local partners, we may pull away from that to address some other threat, but you're always going to have to make trade offs like that.

Budget wise, when I became director, we had a big problem which was sequestration, then we made it worse. We shut the government down, and so we've been digging out of that hole for the last three and a half years. Quantico was shut down for a year and -- and it's hard to turn a university back on, and so we're at the place. We hired 3,000 people last year, we're going to hire 2,500 this year, and what my fondest wish is to be able to sustain those human beings. The FBI is people. We don't have satellites. We don't have aircraft carriers. We are great people, and I need to be able to pay them and support them. And that's what I'll be working for, for the next years budget.

LEITER: We unfortunately only have time for two more questions. And I kind of know where this one's going to go, but about half my packet of cards includes something like this so I'm, just so everyone knows, I 'm not just ignoring it.

COMEY: I'm 6'8".

LEITER: Yes.

(LAUGHTER)

LEITER: I fear that you said that as a threat to me right before I ask this question. Could you comment on your commitment, the FBI's commitment to pursuing to its ends, whatever ends those are, the investigation that you commented on in front of the HIPSY involving Russian involvement in U.S. elections?

COMEY: I don't want to comment on that particular matter. I'll say generally though, what I said at the beginning. We are the same today as we were yesterday, we'll be the same tomorrow. We ask, what are the facts? We really don't care who's political ox is gored by our work and that is the passion at the heart of the FBI. We will always be that way, and that can make us annoying in different circumstances. I hope it's comforting to the American people. We are competent, honest and independent. We were that way when I was lucky enough to become director, when I leave in six and a half years we will still be that way. I hope that's reassuring to people, but if it's annoying to people, it doesn't matter. We're going to be the same.

(APPLAUSE)

LEITER: Last question and very relevant to many people in this room. Clearly the bureau comprises 30,000 plus U.S. government employees, but is supported by many tens or thousands of people from industry, whether they're providing information technology or analytic support or basic functional support for the FBI. What do you want to see more of? What would you like to see less of? Where do you think you need help from industry in a way that you, as FBI director, can't get the U.S. government to move fast enough to face the missions you have to face down?

COMEY: That's a hard one. I need you all to help us be smarter and better and know -- I talked about that attitude of humility when it comes to cyber. You will find that the commander's intent is in all aspects of the bureau's work. We do not have a monopoly on wisdom. We need you to bring to us smarter ways of doing things, cheaper ways of doing things, faster ways of doing things, and help us be agile. It's hard to be agile when you're 109. You tend to calcify and break a hip, but we are determined to be humble enough, proud enough of our century of achievement but humble enough to be agile. You will bring us the opportunities to demonstrate that agility first.

And second, I really do hope you'll urge your people, especially those who are in place for a longer term contract, to get part of our culture. And one of my concerns is, with long term contractors who don't -- who don't feel part of the FBI and don't act like they work for me, and I know they work for you but I need them to be part of our culture. I have met contractors, some of whom were all in. I met a group at one place where I sat down at the cafeteria to chat with them and they asked me to move out of the way because I was blocking the TV.

LEITER: You are tall.

COMEY: Well they knew I was the Director of the FBI, but they really didn't care because they don't work for me, and that is something we can't have. And I know you as a business model, you don't want that, we need you to be not us, but of us in a way that will help us both be more effective at accomplishing the mission.

LEITER: Well, I'll end where I started. Jim has what, I think, we all know is one of the most challenging jobs in the U.S. government, if not the most challenging job other than the President. And, I don't think it's going to get any easier the next six years, but I hope everyone is heartened, I know I am, by the intellect, the integrity and kind of the vision that you bring to this role. And I want to thank you for your past service and thank you for the next six years, because it will not be, we don't know what's going to happen, but none of them will be easy years. Thanks very much.

COMEY: Thank you, Mike.

LEITER: Thank you. Great job.

END