Center for Strategic and International Studies

The National Security Division at 10: Past, Present, and Future

Panel I: The National Security Division's Response to Evolving Threats

Panelists:
David S. Kris,
Former Assistant Attorney General, National Security Division,
Department of Justice

J. Patrick Rowan,
Former Assistant Attorney General, National Security Division,
Department of Justice

Kenneth L. Wainstein,
Former Assistant Attorney General, National Security Division,
Department of Justice

Moderator:
John P. Carlin,
Assistant Attorney General, National Security Division,
Department of Justice

Location: CSIS Headquarters, Washington, D.C.

Time: 9:30 a.m. EDT
Date: Wednesday, September 14, 2016

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

JOHN P. CARLIN: Just repeat the thanks to the attorney general. And we'll now – you can see why it's such a pleasure to serve with her day in and day out for our division. And it was such a pleasure to serve with her as the career prosecutor that she was when she was the head of the U.S. attorney's office in the Eastern District of New York.

And we'll now bring on our next panel. It'll be a panel discussion with the three prior assistant attorney general of the National Security Division.

One of the advantages of only being 10 years old is there would only have been five of us. And so today you will hear from all four predecessors as assistant attorney general. And they're coming out now.

Our first assistant attorney general was Ken Wainstein. And Ken's background was as a career prosecutor. I had the pleasure of first meeting him, I believe, when he hired me as a career prosecutor in the U.S. attorney's office for the District of Columbia. He went from there, and if you look carefully throughout government, Ken's picture is on the wall of, I think, every building, given his jobs around. He was, among other jobs, general counsel of the FBI, chief of staff to Director Mueller. He was the U.S. attorney in D.C. He was an AUSA in the Southern District of New York. He was the head of the Executive Office of U.S. Attorneys. And then after being the head of the National Security Division, he was President Bush's homeland adviser where he was the chief adviser on how to prevent terrorism acts.

We also have with us his successor, Pat Rowan, who is another career prosecutor, who also had worked for Director Mueller at the FBI and worked on intelligence issues for the deputy attorney general and is currently a partner at McGuireWoods.

Ken is at Cadwalader.

And we have with us David Kris, who I think we would all say is the scholar of the group, who has written the textbook on the use of intelligence authorities, and similarly had served as a career both prosecutor and appellate lawyer inside the Justice Department and is currently the general counsel of Intellectual Ventures.

So please join me and give them a warm welcome. (Applause.)

Maybe we'll start off chronologically. Ken, you had the easy task of being asked to be the first assistant attorney general and to create the first new litigating division of the Department of Justice in about 50 years, since the creation of the Civil Rights Division. Can you tell us a little bit how it was to start up a division and to do so in a time of grave threat where it's not as if you could divert resources from confronting the terrorists and other national security threats at the time?

KENNETH L. WAINSTEIN: Yeah, good question. Good to see everybody. And thanks for inviting me to be a part of this. This is a great event and a great milestone.

You know, the startup, everybody thinks, oh, you started up a whole new division and it must have been just a monumental task and you're heroic for having done it. And I, of course, agree with that wholeheartedly, especially the hero part. (Laughter.)

But the reality is it wasn't as hard as I expected it to be, for several reasons. It wasn't as hard for me personally because I –

J. PATRICK ROWAN: It's the story of your life.

MR. WAINSTEIN: Yeah, the story of my life. Other people did the hard work, I took credit for it. (Laughter.)

But the reality is –

DAVID S. KRIS: OK, here we go.

MR. WAINSTEIN: – I got nominated, I couldn't get confirmed for about six months for a number of different reasons. But all the things got sort of put in process. And Charlie Steele, who was the chief of staff, who really was the one kind of pushing the process of building the division from the beginning, he started working. Pat was, you know, plugging away.

So we had people really working hard while I was pending confirmation, fat, dumb and happy sitting out in the U.S. Attorney's Office having a blast. So by the time I got in, actually a lot of things were up and running, so that's one advantage that I personally had.

But really, the biggest advantage, and I know that Alice Fisher is on the agenda for later on today, is that while I think one could sort of assume, if you look at the scenario, that this new division is going to be stood up, it's going to be yanking really important parts of, you know, of different divisions into itself, taking away, you know, really important cases and great staff, that there might be some resentment or some resistance, you know, sort of bureaucratic resistance or maybe, you know, maybe just apathy and that we would have to deal with that. We got none of that.

The Criminal Division stood up big time and helped us out, because really, you know, the CTS and CES, the two prosecuting sections, came out of the Criminal Division. Alice and her team did everything they could to make a smooth transition.

And this is, you know, I actually warned these guys. This is going to be happy talk and sound like it's sort of overly rosy, but it's actually true. We got support from the AG all the way down. So in terms of the logistics and the resources that were needed to stand up the division, I can't think of a single time where anybody said no. And that made all the difference in the world.

So the mechanics of standing the division up, actually, while it was hard work, I think it worked out tremendously well, better than I expected.

John, you mentioned, you know, it was having to do that in a time of, you know, turbulence and change and threat, and that was challenging. But, you know, it was sort of a challenge, but also it was a blessing, it being that we didn't have time to sort of get in place, stand up, focus on ourselves before we actually had to engage. I mean, we were engaging on day one, dealing with the terrorism threat in particular.

But as I say, that was a bit of a blessing, because what happened is we immediately jumped right in, whether it was the Terrorist Surveillance Program, you know, dealing with getting that brought under the FISA Court authority, or dealing with military commissions that had the Military Commissions Act that just passed the month before, or dealing with FBI oversight issues. We sort of jumped right in and our people were able to show their value and be at the table and show they had a place at the table, whether the table was at the Sit Room or in the intelligence community or elsewhere within the department.

And that was a blessing because, you know, we immediately were in the middle of things and people realized, OK, these might be the new kids on the block, but they're adding value. So while that was a challenge, having to jump in, you know, in the middle of, you know, a high-threat period, it was really, I think, where we were able to demonstrate our value and become sort of part of the machinery of government.

MR. CARLIN: So, Pat, you've heard Ken's rather happy description of when I walked in Pat had done all the work, so the division was up and running along with others, and then we never had any turbulence with anyone in the field or between law enforcement and intelligence. Does that description fit with your memories, or are there a few other troubling moments?

MR. ROWAN: I think there was a little turbulence, but we'll let Matt Olsen speak about that at some point in the future. (Laughter.)

No, I mean, honestly, Ken's right. The overall vibe was, you know, this is important to everyone, we're here to support you. I mean, I think what I recall being very concerned about was that with the new division being created, which was sort of the physical manifestation of the wall coming down, it was very important to us that we demonstrate a level of nimbleness and efficiency that everybody would expect from a new division that had both control over OIPR as well as CTS and CES.

And again, I don't think, from my perspective, that this was a turbulent – it didn't create turbulence, but it did create a pressure on everybody, from the people in the front office to all the folks on the line, to make sure that, you know, a request that came in, whether it's from the FBI or a U.S. Attorney's Office, was handled quickly, that we were willing to rethink decisions that may have been made in the past about how to mix and match your surveillance and your other investigative authorities, and that we're, you know, willing to see what we can do to push the envelope a little bit further.

And so there was that kind of an attitude of, like, look, we've got to make sure that we produce even better than folks have been producing in the past. And I think, by and large, we were pretty successful in that.

But Ken's correct that there was terrific support for what we were doing. As soon as people outside – I mean, I think particularly outside agencies appreciated that now they sort of had a little bit more of a one-stop shop. And so, by and large, it was a very positive atmosphere and it was, actually, it was a lot of fun, too.

MR. CARLIN: And – (inaudible) – a question for you. We focused a lot today, and rightly so, on terrorists and spies. I know a project that continues to this day in terms of enforcement focus, that really started under your watch to get additional resources, is export control and how to keep weapons of mass destruction out of the hands who would do us harm. Can you tell us how you saw that fit with the general mission of the National Security Division and what you did to address that threat?

MR. ROWAN: Well, it fit in a lot of ways. I mean, first of all, CES was a smaller, but really elite unit within the new division. And we wanted to make sure that we did everything we could to support them. And one of the things that they were seeing more and more of was export enforcement cases.

And, you know, some of them were spinning out of intelligence investigations where the FBI would pick up information about someone, they didn't understand what he was doing in the U.S. and then they figured out that he's really here just to export technology. And so these cases were out there, and I think what was done with the export enforcement initiative was sort of bringing them under one umbrella.

One of the key pieces was we had different agencies with different ideas about how to do their cases. ICE and FBI both had an idea about doing these cases and didn't particularly like to talk to each other, so part of it was coordinating those. And we had, you know, we brought in a new coordinator to push training out.

I mean, I think one of the concepts here was, look, we have a lot of prosecutors around the country that have been trained in national security investigations. They know how to handle classified information, they're comfortable with all these issues. Some of them are available, let's put them on these cases as well. And so we pushed more of an emphasis out there. And it was sort of an opportunity where there was a lot of pieces in place and it really needed someone to bring them together, and that was ultimately Steve Pelak who we brought in. And, you know, he did a great job and it was a very successful effort.

MR. CARLIN: And, David, you were the first AAG to take over coming in from the outside. You had been out of the department for something like six years. You come in with a transition to a new administration. And can you tell us a little bit about what it was like before and after, from your perspective.

MR. KRIS: Yeah, I had the enormous advantage of coming into a National Security Division that Ken and Pat had set up. And they had gotten the structure, the sort of bones of the system put together. And, of course, being modest guys they play down that achievement and they say that everybody worked and played well together, and I'm sure that's true. But it's

nonetheless a startling thing to build something from nothing. And so it was great for me to come into something that made sense. The org chart was there, many of the people were there, the structures worked.

I remember maybe the most surprising thing to me during transition, because I had been in national security work from 2000 to 2003 and then took a break for a while and came back, was the incredible degree of cooperation that existed between NSD and the bureau.

Those of you who worked in this space, you know, years ago remember some fairly turbulent times, some challenges, and that relationship had just dramatically improved in the six years that I was away. And I think Ken and Pat and Bob Mueller and may others deserve a lot of credit for that. I think, frankly, creation of the DNI and the Department of Homeland Security during that period may have also helped bring the bureau and mother justice together. But whatever it was, that was probably the single-most startling thing to me when I arrived there.

And what I tried to focus on was taking this very well-designed structure that Ken and Pat had put into place and just getting it to work, putting some muscle on the bones, I guess. And I emphasized and was roundly made fun of for emphasizing the idea of synergy between the intelligence side and the law enforcement side of NSD to try to get them to come together and take advantage of the fundamental legal insight that permitted the division to exist in the first place, which was –

MR. CARLIN: I just noticed about a hundred people took a drink when you said synergy – of water, of water. (Laughter.)

MR. KRIS: Somebody's probably playing Bingo.

MR. CARLIN: Because we're national security professionals.

MR. KRIS: (Laughs.) Bingo!

– to fulfill the promise of tearing down the wall. The NSD is the bureaucratic structural analog to that legal change. And, you know, the only justification for pulling terrorism and espionage prosecutors away from their colleagues in the Fraud Section, let's say, is if there is a greater benefit, a synergy from combining them with the intelligence lawyers and organizing according to mission rather than tool or technique. And I think that was what I thought was the idea behind NSD and that was what we tried, I tried to help implement in the couple of years that I was there.

MR. CARLIN: Just a quick review of the number of convictions since the creation of the division. We've now convicted over 340 individuals for terrorist-related crimes. Now, in doing so, we used the criminal justice system, the federal criminal justice system. This may be a jump ball because you've all confronted it.

But I guess maybe I'll start with you, Ken. Does it surprise you that using the criminal justice system to successfully convict terrorists and others became a flashpoint?

And then after Ken addresses that, I'm curious on everyone's thoughts, David, on how you handled that tension where, for a period of time, it was controversial to convict people in the U.S. courts.

MR. WAINSTEIN: Yeah, so that controversy really got kind of white hot after I left. That was sort of later, really more once the Obama administration came in. So as to why it became such a controversy, I think that's more political than anything.

As to the question, you know, is there some reason to question the effectiveness of the criminal justice system, the Article 3 system in prosecuting terrorists, I as, you know, we're former prosecutors here, very comfortable with the Article 3 system and have seen it be very successful against threats over the years, whether it's, you know, I think you can define sort of different threats, the drug war that I came in as a young prosecutor in the middle of, you know, and the use of the courts to try to protect or, you know, to protect the cities of our country against the scourge of drugs. Or it was, you know, using the courts to go after the mob, you know, Robert Kennedy and the spitting on the sidewalk approach. I mean, we've seen it work over and over and over, not perfectly, but it works well.

And you look back at the number of the convictions that you're citing in the terrorism area and it's not surprising. I mean, you look at the actual charges, they carry stiff sentences. There are the tools in the system, which are very effective at identifying and convicting terrorists, like the cooperation process that they have in the criminal justice system where you can, you know, get leverage on somebody and get that person then cooperating against his or her confederates. I mean, it doesn't surprise me that it's been used well against terrorists, you know, for generations, but particularly since 9/11.

And, you know, while we could all sort of go back and forth about whether that's a better system or the military commissions are a better system, at the end of the day I don't ever see a future where we're not using the courts to go after terrorists. It's absolutely critical, obviously for U.S. persons, but even non-U.S. persons.

MR. CARLIN: I think I'll jump to David. Ken talked about how it –

MR. KRIS: It was pretty hot during my time, as I recall. And so I did what I normally do when confronted with a challenging political issue, I wrote a really long, nerdy, law review article that no one read. (Laughter.) I mean, the argument, as I understood it, was, you know, this is a war, our adversaries in this war are not common criminals, so we ought not be using these criminal tools that we use against people who have robbed the corner liquor store, against them.

And my view in response to that was, this is war. In war, your goal is to win. And it turns out, when you look empirically at the data, law enforcement is a tool that helps you win. It is a platform for disrupting terrorist activity, for incapacitating terrorists for the long run, and for gathering intelligence from them, often in exchange for, you know, reduced sentence, as is traditionally done in the criminal justice system. And it's been profoundly effective. And I did,

in the appendices to that law review article that nobody's read, publish a lot of data. And it took a lot of work to get everybody to declassify all the data about both the number of convictions and sentences, and also the intelligence collected through that platform, and it certainly persuaded me. The issue seems to have died down somewhat, although it still flares up from time to time, typically in the context of Gitmo. I think – but the data continue to trend, it seems to me, in favor of validating the effectiveness of the criminal justice system, again, as a platform for disrupting, for incapacitating and for collecting intelligence from terrorists.

MR. ROWAN: John, I just – one thing I did want to say about this is, it – Ken's right; it was political. But I was amazed at the traction that the argument got at the beginning of the Obama administration. I mean, I'm sitting in my law office with nothing to do, and I get these phone calls from reporters, and they're saying – you know, they're talking about taking this guy to the criminal court as if that hadn't been done, as if we hadn't, you know, published lots of lists that talked about all the criminal convictions we had gotten. And so I was – I was surprised. In – I mean, I've been very involved in the commissions. I thought the commissions were in the best shape they were in at the end of the last administration and that they might actually become an effective tool. But even so, it was amazing to me to see the blowback.

MR. CARLIN: As we move to confront cyber – national security cyber threats, some of that debate, I think, has recurred. And people have asked, for instance, why did you bring criminal charges against five members of the People's Liberation Army? They're in uniform. Kris, as to your thoughts now from the outside – apparently doing nothing while making large amounts of money. I never knew that was the private sector approach.

MR. KRIS: We will explain it to you after you leave. (Laughter.)

MR. ROWAN: It's a little slow when you've been doing terrorism stuff for a few years and you go to a law firm, because the terrorists aren't calling you. (Laughter.) Because David's, you know, eavesdropping. (Laughter.)

MR. CARLIN: But I was curious what you think of applying it in this – in this context against what is a new – a new threat.

MR. KRIS: Well, I do think that, you know, you can sort of identify four phases in the national security division's life. The first phase is the precursor, where the wall comes down. The second phase is where Ken, Pat, and Bill did. I think the third phase is a little bit where I was there doing the sort of basic terrorism cases, Zazi, Headley, Shahzad, Abdulmutallab, and then the Russian spy cases.

And I think this fourth phase, John, that you and Lisa have presided over does involve cyber. I think it's very interesting. One of the areas where I think there's going to be a lot more room for the use of law enforcement is what at least I perceive as an increasing level of cooperation between state actors and non-state actors in exploitation of cyber vulnerabilities. There's essentially now a pretty well-developed online marketplace for malware and exploits, and pretty clearly a growing level of cooperation between private sector and adversarial foreign governments. We're seeing a lot of that in the news of late, I think. And so one technique is to

indict to PLA, or its individual members. I doubt you'll get your hands on those guys, but it still can be a valuable tool, and it did seem to provoke some favorable responses. But especially to the extent there's cooperation between government and the private individuals out there, I think the law enforcement system is going to be – and remain – an important, you know, arrow in the quiver.

MR. CARLIN: Ken or Pat?

MR. WAINTSTEIN: I concur.

MR. ROWAN: Yeah, I've been very impressed by what appears to be the impact of those prosecutions. And my take, at the end of the day, there's a lot of people rolling around out there that would like to be able to travel internationally at one point or another in their lives. And so I think it has been helpful.

MR. CARLIN: One job, as assistant attorney general – and this is something that 9/11 in its anniversary report highlighted – is an obligation to explain to the American people what the – what the threat is and what the tools are that we're using to address it. And at the same time, I know I've talked to each of you about what the terrorists are trying to do is use sometimes small-scale attacks to inspire a greater deal of fear than they're actually capable of imposing through consequence. How do you balance not alarming people, overly alarming people or scaring in a way that the terrorists want, with your obligation to make clear what real threats are?

MR. WAINSTEIN: Do you want me to start with that? OK, well, let me break this down on two different threats. Let's talk about terrorism in a second, but I want to sort of use this as a segue for the last question about cyber. I think one of the things that you and Lisa have done very effectively is getting the word out and impressing people with the seriousness of the cyber threat, and I think there are a host of reasons why, frankly, we as a country and as a government, we were slow to meet the cyber threat, partly because we were sort of focused on the traditional kinetic 9/11 threat that we were facing in the years after 9/11 at the time that the cyber threat was building. But I think in that situation, you recognized the need to bang the drum to get people to realize – whether the people are Congress, the executive branch, the American people – that serious measures are needed to meet that threat. And I – so I think that's a situation where you don't need to be so constrained in the strength of the message that you're sending out.

In the terrorism context – and of course we're – we come in in 2006; we're there for the balance of the administration – you know, people were very focused on terrorism as a threat. We didn't need to make people realize it was a serious threat. The wounds of 9/11 were still quite raw. And there – I think there was a sensitivity on our part, and on the part frankly of the whole executive branch – and I saw this once when I went to the White House – that you don't overplay it, especially not for political reasons.

But at the same time, I think the – and you and I talked about this the other day – there – it was very effective to remind people of the seriousness of the threat at that moment when the executive branch is asking for, let's say, a certain authority. And the best example of that was in the run-up to the FISA Amendments Act, FISA modernization, where there was a real need.

And I think everybody would agree, or most people would agree, looking back, that there really was a need to revise FISA so that our electronic surveillance authorities and capabilities were better able to meet the threat. And in order to get the political will to do that, we needed to remind Congress and the American people that the threat was real. Because, you know, 9/11 had happened. Just as human beings always do, after time, you get a little complacent, a little less concerned. There were the occasional attacks here and there, the occasional homegrown terrorist, but it wasn't front-of-mind. And so it was important in 2006, 2007 to remind people that, yeah, while we'd put a hurting on al-Qaida after 9/11, it was still there. It was actually franchising around the world and becoming more effective in that manner, and that was a message that was very intentionally sent out. And I think that helped to tip the scales in Congress for us to get the FISA Amendments Act. Is that a sort of political use of threat messaging? Maybe. But it was – so long as you're being honest about it – and I think the administration was at the time – I think that's fair. And so I think that's an example, and cyber is an example of where the messaging has been effective and honest with the American people.

MR. CARLIN: And, David, I would – a question for you on that. There was a series of disclosures of some information in 2013 – you may or may not recall.

MR. KRIS: Nothing's coming to mind.

MR. CARLIN: To mind. And as part of that, there was a national debate about the use of an authority, the so-called 215 authority, and it was something that, as you'd presided over but not been able to talk about publicly when it was originally briefed to Congress. And I was curious as to your – what do you think happened with that debate? Part of that debate included an accusation that the use of 215 was lawless, or that NSA had been acting outside the law. I just wanted to get your thoughts on that phase.

MR. KRIS: Yeah, the – this is another challenging issue on which my default response kicked in, and I wrote a long law review article that no one read.

The best encapsulation of that – I – of that issue that you're pointing at is an exchange that occurred, I think, between Bob Litt and Chairman Goodlatte during some of the post-Snowden hearings about this, in which – you know, Goodlatte said to Bob Litt, look, you know, you had briefed the intelligence committees of Congress repeatedly. You had, you know, gotten judgments from, I don't know, 30 times, 40 times from the FISA court for multiple judges, and a briefing had been offered to every member of Congress, and some of them had actually taken advantage of that briefing opportunity before they reenacted the Patriot Act. You had all this discussion going on within all three branches of government. All three branches of government had pretty clearly signed off on the legality of this. What – you know, why would you think you could keep that from the American people? And Litt responded, well, we tried. (Laughs.)

And to me, that's really the debate that was – that's in play over the disclosure of 215. It wasn't the legality of the program per se, because judges had signed off, Congress had reenacted, briefings had been done and offered, and so forth. You know, it was more the question of why couldn't everybody in America know about this? And I think we have seen, in the aftermath of all of that, a pretty serious recalibration of the transparency of our foreign intelligence

surveillance, and with it, I think, a corresponding stepping back in the scope of that surveillance. And that's the kind of recalibration that has to occur from time to time in a democracy.

And we'll see sort of where it goes. I'm in my own mind not totally clear on where the logical endpoint is on this new regime. Are we going to be, for example, as transparent about issues embedded – legal issues embedded in covert action? We have not so far, but it's not totally clear to me why we're going to stop at SIGINT. So I think we're still working through this conversation as a country, and we're going to have to see how we strike the balance between more surveillance or less, and more transparency or less, and in this field and other related fields. But the debate really was not about the legality per se, but more about the transparency to the public as opposed to the Congress and the courts.

MR. CARLIN: Any additional thoughts on that? Ken or Pat?

MR. ROWAN: That was after our time. We didn't have to worry about these disclosures.

MR. KRIS: Yes, I was very grateful to be in the private sector during that period as well.

MR. ROWAN: I think it is true that in connection with that – again, on the one hand, I was surprised at the beginning of the administration about the traction that the argument we should never be in the criminal courts had. With the electronic surveillance debate, I was mildly surprised at how quickly the providers seemed to be able to get the upper hand in that debate. And, you know, that was, to me, you know, again, one of these things where I assume at some point the pendulum may swing back, but I was surprised that there seemed to be such widespread acceptance of the position they took about privacy versus our ability to conduct surveillance.

MR. CARLIN: Let me switch a little bit and see, running through it chronologically, but what accomplishment or success are you most proud of during your tenure as assistant attorney general?

MR. WAINSTEIN: You know, well, sort of standing up division – just to make it clear there was a heck of a team. We had a really good team. Matt Olsen, I know, is here, and Brett Gary (sp), and John Murrs (sp), and Pat, Charlie Steel (sp), and many others.

And, you know, so we – that was, you know, probably first and foremost the thing that I think I'm most proud of. And as Pat said, by the way, it was a heck of a lot of fun. When I talk about most sort of just satisfaction or pleasure I've ever had in my professional career, it's that period of time.

But there are a couple of things that I think I'm very proud of. Look, the – Pat sort of alluded to it. It – the whole electronic surveillance issue was front and center, and we needed to sort of get – establish ourselves in that area. We have taken the OIPR, now the Office of Intelligence, in, and have it be integrated in. And this was Matt Olsen's – his job, and he handled it magnificently.

But at the same time, establishing a relationship with the NSA, which was really important because we were going through a lot of changes in terms of – in terms of surveillance and the authorities.

And then the – getting the FISA Amendments Act across the finish line. That was a huge help. And obviously many people in government were involved in that, but our folks played a really central role in that. And that, of course, took place after the department, OLC, and we and others got the Terrorist Surveillance Act under the FISA Court authority, which was a key step in that FISA modernization process. So that was tremendous.

And I guess the other thing that I would say was I think a credit to the department and also the FBI is that in 2007 we stood up a much – an enhanced oversight capability and section that had direct oversight responsibility and authority over the FBI's national security investigations, which is sort of a first in history. And the FBI stood up and said, yep, we want this, we'll work with you. And I think, you know, my sense is that's been a real success and has given – has been one of the things that's helped to give comfort to Congress and the American people that these investigations, which are using pretty strong investigative authorities, are being conducted responsibly.

MR. ROWAN: I feel silly talking about competence with all the people in this room because anything that I did was basically just signing off and approving what they had come up with and what they were working on. But I think, you know, the thing that I'm most pleased about, one, that the division was operating as well as it was when David came in – that David was in a position to say, hey, this seems to be working OK. And we – the whole transition period was very interesting and really heartening to me because there had been a message from the White House on down, OK, look, national security transition has to be top priority, it has to be done right. Give everybody what they need. Let's make sure there are no – there's no problems. And that's exactly how it went. It was a – it was a very, you know, as I say, heartening thing to see. But I was very happy that – you know, I remember sitting down with David towards the end. They had – the transition team, which David was a part of, had done a lot of work. They had poked around. They had looked under the hood here and there. They had asked a lot of questions. And then, you know – you know, I got the sense from David that he had not found any huge problems that he was going to have to tear his hair out about on day one.

MR. KRIS: That had already happened, evidently. (Laughs.)

MR. ROWAN: Yeah, I guess I understand that would have already been something you didn't have to worry about. But anyways, so I was, you know, heartened by that. And that whole period was – as I say, it was – it was terrific to see how everybody worked hard to make that work, and that, you know, what we turned over was what I think the people that passed the legislation that created the NSD would (agree ?).

MR. KRIS: I'll just riff off of that for a moment. I was involved in transition when the George W. Bush administration came in, and then from the other direction as part of the Obama administration coming in. And I remember getting some advice from David Margolis, who was a mentor to me along with so many others, that the biggest mistake transition teams make when

they come in is mistrusting anyone who prospered under the prior group, whether they are career or political. And I thought that was very true. And I would say I agree 100 percent with Pat that the reception we got coming in at the beginning of the Obama administration at DOJ was just spectacular, and the support was genuine, heartfelt, thorough, complete. And we really, you know, got the benefit of the learning of the people who were in the seats that we were about to occupy, and it was enormously helpful. And I just – I hope whatever the next transition that occurs in a few months will be as smooth.

In terms of, you know, achievements, as Pat said, it's things that happened when I happened to be there, from '09 to '11. Things that I recall fondly, thanks to many years of therapy and medication, I guess – (laughter) – a string of terrorism cases. I mentioned some of them – Zazi, Headley, Faisal Shahzad, Abdulmutallab even – where the – to my way of thinking, anyway, the division sort of fulfilled its potential, where the intelligence and law enforcement sides did work together the way they were designed to work. I was – I was very proud to see our people contributing to that. And then, on the espionage side, the Russian spy case was something that I was very happy and proud to see going on while I happened to be in the chair. And you know, those are probably the memories that I sort of cherish most from that time, are those insane late nights working those cases and just seeing the division doing what it was designed to do. There was a lot of satisfaction in that for me.

MR. CARLIN: Maybe we'll open it up to some questions from the audience. While the mic gets passed, I'll ask you one more to follow up on what you said, David.

But there's been a debate now when it comes to cyber-enabled espionage that says, well, everybody commits espionage, so if it's – if we do cyber-enabled espionage and they do cyber-enabled espionage, shouldn't you give it a free pass? And I'm wondering your perspective on that as – and each of yours – but as someone who oversaw the Russian spy ring case, what the perspective is from the – from the group it tasked with catching spies.

MR. KRIS: I mean, I guess I think everybody does do it. Espionage is not a new thing. On the other hand, everybody also does tend to prosecute spies. (Laughs.) So if you – if the question is, you know, should we just accept espionage and decriminalize it, I guess put me down as a no vote on that. (Laughter.)

MR. CARLIN: Any other thoughts?

MR. WAINSTEIN: No vote. (Laughter.)

MR. KRIS: I think we have unanimity.

MR. CARLIN: All right, questions? Is there someone with a mic?

Q: Hi. (Off mic) – with The Washington Post.

Thank you, John. That was a great setup for my question, which is in the area of cyberespionage and deterrence. You laid out an impressive list of actions the U.S. government

has taken to deter nation-state actors and cyber – malicious cyber hacks: sanctions against North Korea for Sony, indicting the five Chinese PLA officers, indicting the Iranian actors, and you just now mentioned cyberespionage. Is now time to take some form of action, to have sanctions against Russia, or what is going on in cyberespionage there?

MR. CARLIN: Well, I'll say this. So, without commenting on any current investigation or matter, but more generally, that I think you've seen there was a period of time where folks said cyber-enabled espionage, Chinese espionage, there's nothing you can do about it, it's too hard, they're going to be able to remain anonymous, and this is just the world that we have to accept as the status quo. And you've seen as we've described a little bit today that, through changes made in the National Security Division, across U.S. attorneys' offices, and with the FBI, we said no; that with hard work you can do the investigation and attribution, you can bring it public through the use of our criminal justice system, and you can look to impose consequences, whether in the form of an indictment or convictions, such as an individual name Su Bin, who was convicted on U.S. charges after being held in Canada, waiving extradition, and now has been sentenced in the Central District of California. Before we did it, people said, well, the nation-state actors from China will never be caught. And now we've done it.

Similarly, when it came to destructive attacks against our values like you saw North Korea commit against Sony Pictures, people thought you wouldn't be able to figure out who did it; if you did, you wouldn't make it public; and that there wouldn't be sanctions. And they were wrong.

And when it came to the Iranian attacks, denial-of-service attacks against our financial sector, their intrusion into the Bowman Dam, actors affiliated with the Iranian Revolutionary Guard Corps, we showed there by name, by face that we could bring charges to hold people accountable.

So whether it's Iran, North Korea or China, there was a before, and then through hard work by folks in the National Security Division and elsewhere, there was an after. And you've seen that with Syrian Electronic Army, you've seen that with hackers associated with the Islamic State in the Levant. So those who think that – be it Russia or any other country – that there's going to be a free pass, that we can't figure out what they're doing in cyber-enabled espionage, I think the message should be clear: you're wrong; you can and will be held accountable; and that, as the attorney general said our memory and our reach is long.

Q: Great. Just to clarify, so even with cyber-enabled espionage, which is an action for which the United States government has never indicted or sanctioned any nation-state before, you wouldn't rule that out with Russia, and would say that it might even be advisable in this case?

MR. CARLIN: So, again, I'm not going to comment on the – on any current investigations. And also, given the good training I've gotten from my three predecessors, I will take issue with your – some of the assumptions in your question.

I think we have prosecuted people for cyber-enabled espionage and we have prosecuted – brought charges against people linked to nation-states responsible for cyber-enabled espionage, whether it's stealing secrets from Boeing, whether it's economic espionage against the PLA. We've done it for people that have stolen information digitally, and we've prosecuted people, as you know in the real world, including traditional spies. Great case out of the Southern District of New York involving a Russian spy named Buryakov. So I think, as David was eluding to, although people spy, it has long been both through the 10-year history of the National Security Division and our distinguished history before that that led up to it of the espionage prosecutors, that our prosecutors and agents, if you get caught spying, there are consequences.

Q: Hi. I'm Carrie Johnson from NPR.

It's quite something to hear several of you speak openly now about some of the early controversies in this administration being attributable to politics, and also being surprising to you. Pat, you said at the end of your tenure you thought the military commissions were in as good a shape as possible, and you thought they might be an effective tool. The record demonstrates that hasn't been borne out, at least over the last seven years. If any of you gentlemen were in power now – and John, to the extent you can speak to this too – how do you un-ring that bell? How do you fix that problem?

MR. ROWAN: That's why you don't run for president. (Laughter.)

I think it's really hard. I mean, I – you know, we had a great shot in the military commissions at the end of the Bush administration, I thought, and we had a second great shot when they were set to bring the 9/11 conspirators to New York. And I'm not sure where the third shot comes from. I think, you know, I'd have to muddle along.

MR. WAINSTEIN: Yeah, I think actually, historically if you look back at it, you know, the president issued the executive order, I want to say, November of 2001 standing up the military commissions and then went through sort of the tortured history after that. Had they been stood up quickly or even at a reasonable pace, the rules been put in place, people would have actually been processed through the process. It would have become sort of a standard exercise. Then I think we might well have had a successful process.

As David argued in one his long, boring law review articles, which I did read – (laughter) – I didn't think it was that boring –

MR. KRIS: (Laughs.) Thanks a lot.

MR. WAINSTEIN: – you know, look, it's always better to have more tools than fewer tools. And looking at it from the perspective of a prosecutor, having both the Article III courts but also military commissions was helpful and would be helpful, and it's a shame that it's – that the military commissions are where they are right now.

Q: Thank you. Victoria Feinberg (sp), retired from the Department of Defense. (Inaudible.)

I recently attended a seminar at the FTC about ransomware. And ransomware today is a very large industry, with multibillion-dollar revenues, industry that has its own developers, so their own code, with their own customer service. And the revenue's growing exponentially. What can you do to disrupt this very powerful industry? And this is cyber ransomware.

MR. CARLIN: Yes. So I think the question was, given the growth of ransomware and the fact that it's so lucrative, which then fuels additional use of ransomware, what can you do to address it? And just a brief definition. I think people tend to use ransomware broadly, so this would be the idea that you can deliver code onto somebody's computer and it makes it so that the person can't access their information. And because they want to get access to their information again, then the crook or the spy or the terrorist says pay me X amount of dollars if you want to be able to see your information again. And we've seen this used for really commercially important information, but also for things like medical data that could have life-and-death consequences. And to design it a little more broadly, I think you've also seen extortion that doesn't involve the code that would encrypt the contents of your information, but instead – same idea of ransoming – says I'm going to release embarrassing information that I've stolen if you don't do X or Y.

MR. KRIS: I haven't studied this problem too extensively, but I guess my sense is, you know, of course there's lots of things people should do to secure their data, to back up their data, to have the latest virus and updates and yadda yadda, that stuff. But I think the way to attack this – and I think the way you're probably going to see some legal change over the next few years – is on the other end, with respect to the payments. And as I understand it – again, without having studied it too extensively – is that, you know, fintech is what is enabling this, cryptocurrency.

And I personally would not be surprised to see over the next few years increasing regulation that maybe makes it more challenging for these kinds of anonymous, substantially untraceable – I don't want to say it's completely untraceable – payments to be made. Because if you're making a cash exchange or, you know, credit-card billing, or writing a check to your – to your extorter, you know, you follow the money. It's a traditional investigative tool, and you can do that. But so I think probably where you're going to see legal change is in the area of the payment scheme. That may be wrong, but that's sort of what I expect.

MR. CARLIN: I think we have time for one last question.

Q: Hi. Mieke Eoyang from Third Way.

Yesterday, Undersecretary of Defense Marcel Lettre talked about provider access to information with the government, and said the best way for the government to get access to information is to have quiet conversations with email service providers, telecommunication providers. I was wondering, do you think the Department of Justice will continue to seek to compel companies to cooperate and provide technical assistance to the government to be able to get access? And if not, what's the best way for the government to improve its technical capabilities?

MR. CARLIN: I'll let others jump in, but more broadly, I think you've seen since the dawn of our republic and our Constitution that we've set up a regime that allows for – that codifies the protection of privacy of, say, our homes and our personal papers, but also provides a means with a court order and requires a court order and a certain finding that the government with that court order is entitled to that information, and has oversight from that other branch. I'd be surprised if we change that fundamental – that fundamental commitment that we've made through our Constitution as to how to tackle this problem. And so what we're seeing instead is a way to apply it in a world where technology is suddenly changed very quickly, and to see when a court order might be appropriate.

The other side of that equation I think was just touched on when it comes to national security, cyber threats, is the cooperation that you get from victims. And the other thing that we're in a process, I think, of changing now is, just like in some ways with early organized crime, where small businesses just accepted it as a cost of doing business because they thought they had to pay off Cosa Nostra and there was no point in going to the authorities, we have private companies, the vast majority of them throughout the United States who are the victims of crime don't report it. Instead, they'll do things like pay off ransomware. And in order to change that calculus, we need to show that there are results when you do report it – there are benefits. And we need to change our conversation in a way where we don't blame the victim for being the victim of a cyber-enabled attack, but instead we blame the bad guys who did it, be they crooks, terrorists or spies.

Other thoughts?

MR. KRIS: I mean, Mieke, I'm not familiar with the remarks, but just in general one of the things that I think is going on right now in the post-Snowden era and after the way the administration responded to that as well is – I mentioned earlier I think there's increasing cooperation between the private sector and government in certain unfortunate areas – Dark Web, malware exploits – and the increasing marketplace there that's, I think, lowering barriers to entry for high-level cybercrime. On the flipside, I think has reduced cooperation between the private sector and the government, you know, in the United States. And I think the providers have been fairly – not fairly; they've been quite explicit and proudly proclaiming that they will not cooperate unless compelled to do so.

My perception – I don't work for a provider – is they want to be compelled. They want to be able to say that they don't cooperate except where they're compelled to do so. And so I think you're going to see a lot of the debates that we're facing right now, whether it be encryption or certain other things, playing out under the rubric of the technical assistance provisions in FISA and in the Wiretap Act and so forth.

So my perception is the days of the quiet conversation and the secret voluntary cooperation maybe not over, but are much reduced from where they were. And the new dominant paradigm, because of the reaction to the Snowden disclosures and the reaction to the reaction, is more towards compelled assistance under law pursuant to court order and then, in certain cases – not all, but in certain cases – the providers going to court and fighting, as you saw with Microsoft, for example, in the Ireland case and Apple in San Bernardino and so forth. So I

think, if anything, the trend is more towards compulsion and then fighting in court over exactly what are the contours of that – of that compulsion.

MR. CARLIN: Please join – we have to wrap there due to time. Please join me in thanking this distinguished group. (Applause.)

(END)