Securing the Courts: Exploitation of the Judicial System by Foreign Adversaries

A Conversation with Giovanna M. Cinelli, Jamil Jaffer, Harvey Rishikof, and Camille Stewart. Moderated by Dr. Samantha Ravich

MAY: Afternoon everyone, and thank you so much for coming. Welcome to the Foundation for Defense of Democracies. I'm Cliff May. I'm FDD's founder and president, and I'm pleased to welcome you today to our conversation, *Securing the Courts: Exploitation of the Judicial System by Foreign Adversaries*. I want to particularly welcome Judge Royce Lambert, who's with us today. He is a 2016 winner of FDD's Alberto Nisman Award, so we're particularly pleased to see you looking so well. We're pleased today to host – Thank you, yes. Give a hand to Judge Royce, a shout out here. Thank you. Great admirers.

We're pleased to host today's program as part of FDD's Center on Cyber and Technology Innovation, which seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. Today's modern economy is deeply threatened by the ongoing massive theft of core American private sectored intellectual property by foreign adversaries, most notably People's Republic of China. An important but significantly under-reported aspect of this threat is the leakage of national security related technologies to foreign actors through our bankruptcy courts. Adversaries are exploiting the U.S. legal system to turn risks to economic security into critical national security threats.

This is an important topic that FDD's Transformative Cyber Innovation Lab has been tackling and we are proud to bring together today's panel to dive deeper into this issue with our co-sponsors, Morgan Lewis and The National Security Institute at George Mason University's Antonin Scalia Law School. Thank you for your partnership. Samantha Ravich, CCTI Chairman, will moderate today's conversation. Samantha also serves as the Vice Chair of the President's Intelligence Advisory Board. Also, was a member of the congressionally mandated Cyberspace Solarium Commission and she also serves on the Secretary of Energy's Advisory Board.

By way of housekeeping, I should note that today's event will be live streamed, is being live streamed. I encourage guests both here and online to join in today's events. You can talk about it, comment on it on Twitter, which is just @FDD. I'd also ask that you silence your cell phones at this time, and with that Samantha, I turn it over to you. Thank you.

RAVICH: Well, thank you. Thank you, Cliff and thank you all for coming out. So about a year and a half ago, FDD, with Cliff and Mark Dubowitz, we launched the Transformative Cyber Innovation Lab to kind of tackle the hardest whole of society cyber issues. And in a conversation with Dr. Michael Hsieh, who's the Executive Director of the lab, formerly of DARPA, it came out that there is serious technology leakage happening out of our bankruptcy courts. We didn't really know how big a problem this was. We didn't know whether anybody was tracking it, but we felt that there was a "there" there and a very critical "there" there.

We brought in Camille Stewart to kind of dig into this more deeply, to understand the scope and the scale of the problem, what laws, existing laws and regulations might be able to close these loopholes, what else might need to be done. She wrote a phenomenal paper. There are copies outside. I hope you all have seen it, *Full Court Press: Preventing Foreign Adversaries*

from Exfiltrating National Security Technologies through Bankruptcy Proceedings. Identifying the problem is clearly the first step. First, recognize you have a problem, right. But at TCIL, at our lab, we don't just identify problems, we look for legal, regulatory and technological solutions to these problems, many of which we're going to address today.

So let me introduce very quickly the panel and then we'll get really right to the heart of the matter. Giovanna Cinelli is a partner at Morgan Lewis working with clients in the defense and high tech sectors on a broad range of issues affecting national security, including CFIUS and export enforcement. She is a true force of nature.

CINELLI: Thank you.

RAVICH: And we are really fortunate that she has joined with us on this effort. Jamil Jaffer is the Founder and Executive Director of the National Security Institute at George Mason. As Cliff just said, he previously – Jamil has previously served in a variety of government roles including as the Chief Counsel and Senior Advisor for the Senate Foreign Relations Committee.

Harvey Rishikof is Senior Counselor of the American Bar Association Standing Committee on Law and National Security and advisor to the Harvard Law Journal on National Security. If you don't know Harvey or know of his work, you really kind of don't know anything because you really have to. And our very, very own Camille Stewart is an attorney working at the intersection of technology, cyber and national security and foreign policy issues. Camille is also a member of FDD's National Security Alumni Network, which is how we were originally introduced. I know we have a few other alumni in the room and I would encourage other mid-career professionals who haven't yet participated in the program to pick up a pamphlet and check out upcoming opportunities.

First, we're going to start with the scale of the problem, then we'll move to discussion of potential solutions and then we're going to open it up to Q&A to focus on what you all want to focus on. Let me start with Camille. In your paper, you identified a number of cases where companies backed by nation state actors acquired sensitive technology. Talk us through how this happens, how you've seen this happen, share a couple of maybe the stories that you discovered during your writing in the paper and research.

STEWART: Yeah, so thank you all for coming out today, looking forward to this discussion. Imagine you are an innovator who comes up with a brand new microchip. It's faster, smaller, more powerful than anything that's on the market. And as you conceive of it, it'll go into a cell phone. You start to build the capability and try to get it out into the market, but you run out of funds. And so to recoup on that investment, you turn to bankruptcy to try to get some of your money back, to sell off the capability, hope somebody will take it further and to start your next venture. You just want to get out from under the debt, and so you are willing to sell to the first person that comes along. The technology you created, although conceived up for cell phones, is such a powerful chip that it could go into weaponry, et cetera. You kind of know that, but that's not the market that you're in at the current moment.

This is actually something that happened in the ATopTech case. They sold their capability to Avatar Systems, which was a Chinese backed company. Actually one of their competitors and accreditor synopsis tried to raise a red flag and say, "There are some problems here and maybe they should go through CfIUS review." That was shut down. Avatar filed a protective order that quashed their ability to raise issues in the case and ATop was sold off to Avatar. Can you imagine that capability unchecked and moving in the market and into the hands of foreign adversaries? That chip implanted in ISCADA systems, ICS systems, weaponry, your cell phone, having a nexus to a foreign actor that we are not tracking, right? That's a huge supply chain implication that could lead to a potential cyber-attack.

Another good example is Molycorp, the sole rare earth mineral mine in the United States. That is really important because rare earth minerals are essential to military and technology capabilities. This mine was in 2015 going through a bit of trouble and almost went up for bankruptcy and DOD stepped in to support it. But in 2017, went up for bankruptcy again and was sold off to Shanghai Resources. The mining rights for the sole, rare earth mineral mine in the United States was then sold off. So we purchase all our rare earth minerals from other countries and the predominance of that from China, particularly in the advent of this sale, which is coming up again now as the Pentagon asked for funds to mitigate this threat. The access to rare earth mineral mines as essential and has become a bartering chip in the U.S./China trade negotiations.

This kind of illustrates how bankruptcy, a hallmark in our innovation ecosystem, has become an Avenue, not only for foreign adversaries to acquire these capabilities by being party to a sale, but also just the observation of it in an open courtroom. We've also seen cases where whether because the folks party to the proceeding have not requested a protective order or requested an in camera review, sensitive schematics or other information are displayed in open court, put into filings, et cetera, and folks can observe an open court, pull the filings, be a creditor in a creditor's round table, et cetera, and get access to a bunch of really sensitive technology.

RAVICH: Yeah, that's great. Following up on that point Giovanna, and first of all thank you and your firm for co-sponsoring this event, but you had mentioned when we were talking before that there's a similar case that starting, has percolated even as late as last week. So if you could mention that and then also picking up on what Camille said about how is this information on technology actually displayed in open court? Because I don't think a lot of people understand exactly how vulnerable we truly are in this regard.

CINELLI: Let me also second how happy I am to be here. I appreciate this is a topic near and dear to my heart. I've practiced for 34 years and I was also a judicial clerk and so saw it from that perspective as well as through the practice. The case that you're talking about is the Doctor Peng and inTouch case. And it was interesting there because a couple of years ago, Dr. Peng came in and bought inTouch, which is a telecommunications firm, and at the time that that happened, that would have been subject to CfIUS review, although there was not a mandatory filing, but it was also required that FCC licenses needed to be filed because there was a change in ownership. Neither of those circumstances happened. Over the course of the last few years, Dr. Peng has been put into financial distress. There's been changes in China with respect to outward

bound investments, so they are now in bankruptcy and going through the bankruptcy process. Their assets are up and there is discussion about transferring the asset to another Chinese company.

But of equal importance, Dr. Peng has been involved in the establishment of the Hong Kong to U.S. cable that Google and Facebook and others have been funding them to build and questions exist about what type of technology did they obtain, not only through inTouch, what will happen if a second Chinese party comes in through a bankruptcy proceeding and separately there may be bankruptcy proceedings in China that could expose information through that proceeding. So that's a case that's currently winding its way through the system. I did want to mention because Molly Corp is an interesting example. Many of you probably remember, in 1995 Molycorp was sold. Again, the mine was unable to sustain itself. There was a critical need from Defense Department perspective, but there just wasn't enough volume and given some of our other laws, such as environmental requirements, was very costly to maintain the mine given that output. And frankly, in that time period we were looking at the inception of the age of information.

While there were some cell phones, lots of things were still fax machines and hard lines. Most of the product was used in defense oriented systems, guidance systems for missiles and submarines and things like that, but there was work being done. Nonetheless, the mine was sold and that capability went away and there was a belief at that time that DOD had sufficient stockpiled capability. That's an interesting technical question about the longevity of a product. Does it deteriorate over time? And that can chemically affect minerals and other substances, which have lives in certain circumstances. So even if you're stockpiling, when you allow something to be sold, either in a bankruptcy proceeding or other item, you're going to have a backend problem given how long you think what you have stockpiled will survive.

But coming back to the court system, we have a premise in our court systems that everything is open. It's very difficult to close a courtroom, not just a bankruptcy court room, but others because there's a presumption that our system of justice should be available to all so that they can understand the issues, the interpretations, the parties that are involved and candidly as a check on the accountability and consistency and accuracy of what happens in the proceedings. It is foundationally one of the preeminent elements of our system and it's what makes the United States an attractive jurisdiction to come and develop technologies and products because the backend of challenges and violations of your rights have an objective system of protection. And even within that system, the courts have for long periods of time understood the sensitivity of some information being publicly shared, which is why as Camille mentioned, there are protective orders and there is in-camera review, but traditionally that has not focused on export controlled information.

It's been primarily a focus on proprietary information. The challenges that, like concentric circles, proprietary information and export controlled information overlap in a large number of areas. So take for example a patent. So in a bankruptcy proceeding, you may have a patent that is in the asset base and the patent is publicly available. Anyone even from Cuba or Iran could access it because it is publicly available information, but the patent by itself, even though it discusses best mode and also enablement technologies, does not present the knowhow

or other trade secreted information that is also part of the asset base. When someone buys these assets out of bankruptcy, they get not only the patent, but they get all the underlying information that is not reflected directly in the patent and that information can be export controlled under one of 28 different regimes in the United States, although the primary ones are the Department of Commerce and the Department of State.

Protective orders that exist in criminal, civil and bankruptcy rules would perhaps be addressed by adding the word export controls as another area besides proprietary information that could be covered more routinely. And there have been a number of cases starting from 1988 with the seminal case of Melvin versus United States, which was a patent on the F-16 and the judge said, "This requires a protective order," and all information was put under the order. And there's been others, the Ross Himes case, the Iridium Bankruptcy case is another one where there have been extensive protective orders with respect to export control technology.

RAVICH: Yeah, no, that's – So as you can tell just from Giovanna just dipping her toe into this, , this is not just onesies and twosies. This is a whole scale problem. And Jamil, when we think about who's on the other side of the equation going after that, I mean, we've written a lot here on cyber enabled economic warfare, but you and the National Security Institute, which I also need to thank because they've been a wonderful co-sponsor in this regard, but you and your colleagues have really written about Beijing's strategy for technological acquisition. So perhaps we can take a step back. What is this all in service of?

JAFFER: Yeah, I mean, look, I mean there's obviously two key aspects to this effort that the Chinese are engaged in. One is the obvious national security aspect, the desire to have technologies and capabilities that meet and exceed our capabilities both in the short run and that they can build on in the long run. But the real – newer play and the one that's actually much more interesting and the one that the President's talked a lot about, the one that I know John Demers, the Assistant Attorney General for National Security is here with us today, my former boss, has been looking at extensively is the economic move, right? Which is to say, the taking – it's the theft of American technology, right, whether it's through cyber enabled means, through the bankruptcy courts, through extorting American companies for access to the Chinese market, that's an economic move, right? It's an effort to take the billions of dollars that American companies invest in R&D every day, every year and repurpose it in China for their economic advantage.

It's a step change in behavior that we haven't seen in the globe until the most recent era. We have known about this now for the better part of a decade. The U.S. government's only been talking about it a little more recently, my now current boss, a former Director of NSA, Keith Alexander, has talked about it as the greatest transfer of wealth in human history. I think that's right. It's an ongoing thing and so it's not just – We've always talked about in the cyber context, right? They're stealing our IP. That's been a common theme of government discussion in the last five to eight years.

But this new sort of era of action, the bankruptcy courts, the extortion of American companies in China to get access to the market, this is another methodology the Chinese are using not just to have access to the national security technology or to have access to

telecommunication technologies they control their own citizenry, but primarily so they can take that technology, give it to their own companies, give those companies low interest or no interest loans, right, essentially state owned enterprises, what we'd call a state owned enterprises in any other contexts, Huawei and ZT to name two, obvious examples that then become national champions.

And now we're becoming, for the Chinese, global champions. I mean, Huawei's dominating the 5G market, not because they necessarily have better technology, the British have told us their technology is actually pretty awful. There are debates about it. There are debates about how much they stole and how much they built on and how good it is, but what is unquestionable is that their dominance is driven in part because their ability to cut prices dramatically. That's a feature of them getting low interest and no interest loans from the Chinese government. And building this on the basis of not having to invest in R&D the way we had to. Unless you think this is just a threat also to big American companies and the large industrial sector, it's not, right. If you think about the modern American economy today, right, we're building our economy on the backs of modern small technology companies that are developing very innovative capabilities, that are then being bought or invested in by large companies and then that's being taken to market.

Those companies depend almost completely on protecting their intellectual property. And if it's walking out the back door, either through IP theft or through extortion or through the bankruptcy courts, well that undermines the entire sort of validity of our new economic transformation. While there are a lot talking about the concerns about our move away from manufacturing and our pivot to technology, right, if that capability itself is undermined, that's not just an economic threat, that's a strategic threat for our nation. That's one that I think it's really important that the current administration has recognized, that economic security is national security. And it's important that the Justice Department is looking at that, that our courts are looking at it and we need to be more cautious in the bankruptcy system and writ large about the threat. It's not just China, but China's the biggest player in the space right now.

RAVICH: Yeah. Harvey, through your work at ABA and MITRE, you see this problem from a lot of different angles and where it intersects, the greater issue of the national security industrial base, the defense supply chain. How does this all fit into that?

RISHIKOF: Sure. So first, let me thank you guys for doing this at FDD and for you and your group and the paper. This is something that we, Jamal said just recently, we have the former Director of the National Counterintelligence Executive sitting there. Many of us have been talking about this issue for quite a long time, but many things in Washington are – It's very much like tomatoes. Something issues are ripe and some are less ripe. This is becoming a very ripe issue and a lot of people are beginning to focus. The tools, our adversaries have a variety of tools in order to gather critical information. And if you think about capitalism, the core to capitalism is innovation. That's what is at the leading front. We used to do studies about who's filing patents, who's doing IP, that's the bleeding edge. How many patent lawyers are in the room? How many IP lawyers in the room? How many bankruptcy lawyers are in the room? Okay. So there's one woman in the back. Usually bankruptcy lawyers are not the most popular people in the firm.

Early in my career, I had did some bankruptcy litigation. The senior partners came over to me and said, "You don't want really want to spend a lot of time in this area, Harvey." Bankruptcy is sort of where debtors and creditors are. People have gone bankrupt. The firm has to think about what's going forward. It's sort of like being spending too much time in a house of ill repute. People think you're using the services if you stay too long. You have to move forward –

JAFFER: Or at all.

RISHIKOF: Oh yeah. "You have to move –" Well, I leave it to you for that. That's sort of the concept that we had. We used to call bankruptcy member judges referees. They weren't Article One. So the point I'm making is that there's a variety of instrumentalities that adversaries have begun to understand that are very, very helpful. Don't just focus on the Chinese. I had a number of Russians approach me, clients, who were arguing that the Russians were using our bankruptcy courts to go after enemies of Putin, declaring bankruptcy issues, bringing their judgments to the United States bankruptcy courts, using the courts to be able to illuminate where all the assets were of the enemy of the Russian state in order to then to try to seize those assets, which is the power that our courts have.

So I start to call this now the F practice, and when I say F practice, I'm thinking of lawyers, usually we refer to as Farrah who do Farrah law, who do FIRRMA or do CFIUS. These are all elements inside the structure that we have created in our legal framework that are starting to illuminate what the actual sources of finance are behind a variety of decisions that are being made by a group of adversaries who are focusing in on wanting to buy, gather, the concept of where the technology is to enhance their ability for them to compete internationally.

It's awkward for us because you know, we always believed in open sources. We've always believed in competition, and now we have entities that are not following our competition rules but are being very effective and the last I will say to you based on the paper that Camille did – I was at the American Bankruptcy Institute annual spring meeting in April. I don't know how many of you have made it, but it's a gathering of the Jedi of the bankruptcy bar and bench and I now have a whole bunch of pen pals from this group who were fascinated by the understanding of what to do and I have one concrete suggestion I'll sort of end with, and one of my bankruptcy new pen pals said, "Look, we understand this is a problem. We were shocked by it. The concrete solution is an amendment to the voluntary bankruptcy petition official form. The form keeps getting more and more complex. In the early '80s, it was essentially, "This company hereby petitions for relief under [chapter X and the code]. Now, the debtor is obliged to disclose as part of the petition whether it has any hazardous waste that might pose an immediate threat in public health and safety." Maybe another item might be added to the position, whether the debtor has the business or assets that could be subject to CFIUS review in a cover."

So there's a concrete way we can use the court and as you said, we're all about at MITRE, the paper that we wrote on compromise, it's all about the illumination of the supply chain. And increasingly, people are approaching me in the private sector saying, "We want to do the right thing," but we ought to know what the tools and assets are that will allow us to do this elimination.

And I think there are a number of instruments we have in the law. As you know, we are talking amongst ourselves, a luncheon group, not to scare people, but you know the War Production Act gives you incredible power from rumination. That ability for you to look and demand from the state and look at these contracts. And this is just part – This thing we're seeing of the bankruptcy, I want to put it into context, there is an array of laws that lawyers usually stay in their silo and they do not understand how our adversaries are using the instruments and these forums help us be able to articulate that.

RAVICH: Yeah, that is fantastic and a perfect segue to the second part of this panel where we're going to talk about solutions. Possible solutions, pathways to solutions. Because here at the Transformative Cyber Innovation lab, we don't only study the problem but we create, refine, to socialize solutions and pathways to them. So let me, let me kick it over to Giovanna.

First of all, do the courts understand that this is a problem on the first hand and if so, or if no, what tools are they bringing to bear in this situation?

CINELLI: So I think like any area there is inconsistent understanding. In some courts, there's quite a sophisticated understanding. So if you're looking at the Court of Federal Claims for example, which deals with a large number of government-related activities in the government contracts area, you will probably find as we did for example in the Ross Himes case that the judges are incredibly sophisticated and understand with a high degree of intuitiveness exactly what is needed.

And so, as Harvey mentioned about the ripeness of tomatoes, I did want to make one observation before I talk about some of the other solutions.

This particular problem has literally probably been around since 1982. There were a number of studies that were published by the old Bureau of Export Administration regarding how joint ventures are established, companies are coming in and taking technologies from nascent industries. There was a focus on China.

In addition, Congress had the Office of Technology Assessment. It used to be their arm to advise them on different activities. Now the Congressional Research Service tries to do some of it, but there's actually an interest in bringing the OTA back. The issue was raised in a report in 1983 and 1987 and then the Bureau of Export Administration raised it again in 1999, as did the National Critical Technologies Council in 1995.

So knowledge was there, ripeness was not. But in those areas there were select cases. For example, the Melvin case in 1988 which was an old court of claims case, which is a precursor to the U.S. court of appeals for the federal circuit. The judges understood that when you have technology that is export-controlled or sensitive for national security purposes, you needed to put it under a protective order.

And that brings me to some of the solutions. So apart from education, which I think everyone, I mean, I'm educated every day by everyone. The situation is so complicated.

But I think establishing an education program for whether we begin with the bankruptcy courts or extend it more broadly through the administrative office of the courts or some other system, providing a resource database that allows them to have one or two pagers that help them identify the issues.

Because unless you have judicial clerks who are particularly attuned to these areas or understand, or the judges themselves have an interest, it's incredibly challenging. So, some form of educational material. And then secondly, some refinements perhaps in the protective order process and in the in-camera review process, because those are areas where it's difficult to address this problem of data exposure once it has happened.

So if you're in an open court and you're looking at an intellectual property case, a breach of contract case, a fraud case, a warranty case, if someone holds up a drawing to try to explain, for example, some piece of IP, and in the corner it says "Subject to the ITAR," the International Traffic in Arts regulation, it's your first clue it should not be in open court. Okay?

And that actually happened in a case in California where, much to the chagrin of the judge, and this was a challenge because neither of the counsel bringing the case had identified it. And yet when they blew it up, you could see right in the corner, this enormous legend about this being ITAR controlled. So needless to say, there were some sidebar conversations after that was brought to the judge's attention.

JAFFER: But it's okay if you block it out and tweet it out? Then it's good.

CINELLI: It's redaction, right.

RAVICH: Just take out the warning.

CINELLI: Right, and it is a downstream matter so the courts can have a protective order, but the second layer there is counsel need to understand that if there's a protective order they can't go and retain, for example, experts who are non-U.S. persons because sharing technical information that's export controlled, even if it's under a protective order, does not address the licensing requirements that they have individually to make sure they don't share the information with foreign counsel, with foreign trade experts or other experts that they need, so some insuring and some specificity in the protective order about the downstream impact might also be helpful.

RAVICH: That's great. Camille, in your in your paper, which again is great and there's a copy out here, you wrote about how FIRRMA is empowering judges to be more proactive. Talk a little bit about that and how that implementation is going and maybe where it can be pushed a little more.

STEWART: Yeah, so there are some real opportunities in the FIRRMA regulation that was released under the NDAA last year. The legislation enumerates transactions that occur pursuant to bankruptcy proceedings and other forms of default or debt as something covered by CFIUS, which is an awesome opportunity and they then charged CFIUS to then create regulations around that.

The first set of pilot regulations were released in November and unfortunately did not touch on these bankruptcy or default on debt proceedings. That said though, they have enumerated 27 NAICS codes which are North American Industry Classification System codes. Thank you. That kind of align a technology to an industry. And they've pulled out 27 that usually align with national security implications.

This was a great flag for judges. One of the questions that we get first, when we talked to them about this issue is how am I to identify a national security related technology? And that's a fair question.

And so, these 27 codes that were enumerated are an opportunity for judges to literally match these codes with the ones that are often included on bankruptcy filings and say there may be, there's a “there” there and we should ask for proof of a CFIUS review.

So that's the first opportunity that comes to light in the pilot regulations and in FIRRMA. Also there are, I'm blanking for a second. There is an opportunity for, oh my goodness.

RAVICH: Too young for that.

STEWART: I know! Okay. I'm sorry. So in the FAQ's, judges need the clarification on how they then make this ask as well as how they manage their docket. Right?

So one of the biggest questions also is if I ask for this, how long is it going to take for this person to come back in front of me? How do I manage my docket?

There is a short form debt filing or short form filing, excuse me, that can be called out so that debt court proceedings, bankruptcy proceedings, can be filed in alignment with the short form filing. So that short form filing has about a 45 day cycle, which is a great opportunity for judges to understand when this person will return to them. They can say, "50 days, return to me with proof of a CFIUS review and we can go from there."

So there are two opportunities that while the procedures as written do not actually talk about bankruptcy and debt court proceedings, they've carved out these awesome opportunities to clarify for judges, clarify for the community ways in which we can understand this problem a little bit better.

And so we've actually been talking to Treasury and they're very receptive to adding these carve-outs, whether to this set of procedures or to the next set in the next pilot. And so, it's been a great discussion to see, you know, the evolution of this, right? They wanted to put their hands around a small chunk of the problem and really understand that when they open the aperture on what things could be filed under CFIUS, what they would get and did not intend to address bankruptcy in this set of pilot regulations, but the way in which they've written it really is right for this kind of a discussion and they're open to that.

CINELLI: Could I make – because you made an excellent point about the NAICS codes, so they are tied to national security. But what I think you're going to find interesting when you

look at the 27 codes, it includes nanotechnology, biotechnology research, ball bearing. Okay yes, you do find tanks and missiles. You do find semiconductor and semiconductor equipment manufacturing. But I think one of the issues, again for the courts to focus on is it is not a very narrow definition of national security. It is now become incredibly broad. It is a counter intelligence activity. And so, in order to intuit where these issues could arise, it's important that these items be understood is not just a very narrow silo.

RISHIKOF: I just want to say that what's fascinating is we never would have had the national security division here 10 years ago. As a matter of fact, I'm so old that we didn't even have a national security division when I was with the Department, so it's actually – I want to commend the Department because it's an understanding that these issues are rising into a national security emphasis and significance. We have the task force being stood up at DOD that's looking at critical sort of infrastructure.

We have what's going on with the bankruptcy courts, but we don't have a real quarterback, one center point, but I think NSD could play that potential role and it'd help to educate also, we have the federal judicial center, we have the administrative office, the federal courts. You guys play a big role in helping to educate. I know the bankruptcy judges want to do this, Professor Tab and the gentleman who is my new pen pal, Mr. Robert Barnes.

So I think it's interesting that this is rising because it's always a great thing when you show up and it's always a bad thing, because it means that serious people in the national security enterprise are saying, "Hey we've got to think about this," because that's why I just want – this is what's commendable and I want to thank you guys for being here, but we need to think through that process both with guys like Baker in the private sector who understand what's going on with their clients and those issues and the bar and I think people at the intelligence agencies, this is a great moment for us to start thinking through to develop a plan to identify what we want to see what the enemy's doing.

RAVICH: And you know, let me just see and get Jamil into the conversation here.

JAFFER: This has never happened before.

RAVICH: It'll never happen again, so.

RISHIKOF: They're so delightful.

RAVICH: Seriously. It has never happened before. How – I mean, how do we equip judges to become more national security experts? It's kind of outside their brief so to speak, but now they are in some ways, again, like so many other players, on the front lines. So talk a little bit about, you know, some of the things that you're involved in, some of the things that we want to go down the path with.

JAFFER: Yeah, I know this is a softball. No, it's great. Thank you for asking the question. We partnered with, with TCIL and with The Law and Economics Center at George Mason University Law School to put together a proposal to one of our funders whose just

generously agreed to agree to give us some money to actually educate bankruptcy judges and to kick off a pilot program with Camille, with the team at TCIL to educate judges in this area specifically and talk about what the opportunities are, what they can do with their existing tools and what new tools they might advocate for within the AO, within to Congress and talk about what tools they need and what tools they can use today, including the protective orders they have the capability to issue today, partnering with their district court judges to recommend things up and push things up to the district court where they need to, to engage with the Justice Department when appropriate, to highlight things or to ask for CFIUS reviewer to at least recommended the parties that they come back and go to the justice department and say, we think we have something that needs review.

So the bankruptcy judges have a lot of authority in this space, in terms of their control of the debtor and they have a lot of room to run and now it's a matter of saying to them, "Look, this is a thing that you should care about," which as Harvey has pointed out and his pen pals have indicated to him that it's something that they do care about.

We had a similar experience. I was with a few bankruptcy judges at Law and Economics Center conference down in Florida, and they were deeply interested in these issues and were excited to hear that there was an opportunity to learn more about it and learn what their tools are. So I think there's an opportunity here that we've gotten now with this donor who's willing to help us support this kind of an effort. And so we'll be out there, we'll be talking to bankruptcy judges around the country. We'll be educating some district court judges.

I think we'll focus in the first instance on the Northeast corridor, Delaware, New York. And then if it works and people find it of interest, we'll expand a nationwide.

Expanding the aperture, this is part of a larger effort that we've got ongoing to educate judges in a variety of fields of law, but in particular for NSI and for TCIL and for our partners, an opportunity to educate judges in the national security and cyber arenas, going to really get them up to speed and give them the tools they need to effectively identify issues in a court room. Think about how to utilize the tools they have where, whether it's CIPA or other capabilities and really addressing some of these threats and lean forward. Even though they have a narrow role to play, it's an important role and one that we think that judges can in doing their day to day jobs really help effectuate the national security.

RISHIKOF: Just for the viewers – CIPA is the Classified Information Protection Act.

JAFFER: Thank you. Sorry, yes.

RAVICH: Harvey, and then Camille before we kind of turn it open into questions, were there other possible solutions that you had mentioned. A form and other things?

RISHIKOF: Just think of the aperture. So you know you said that the judges, this is new. We have one of the legendary judges from the Foreign Intelligence Surveillance Court sitting in the audience. There's been a whole history under the FISA court of the development of judges

who have been extremely skilled at understanding what the threat matrix is coming at the United States.

We carved it out as a separate court as a separate understanding of article three judges. Bankruptcy has always been a separate entity unto itself, which is always intriguing, as Article One judges.

But there's I think an opportunity for there to be an understanding of what the threat is and it's not the traditional threat that we've historically understood of Title 50, spy versus spy surveillance. This is a whole new – that many of us, we've been trying to ring the bell for a long time as you said, since the 80s, but I think there's a huge opportunity for them to understand how are the networks are being created.

And I think there's also a role for the National Intelligence Council and the idea of an NIE, a National Intelligence Estimate, I think it would be very helpful if we went forward to have that and it can be classified to get a greater sense. And where you sit, it would also be helpful to PAB, to help generate that so that we start getting a much better map of what is going on with critical adversaries and that that is then passed out to the judges in a way that gets them to understand. And then we reform the forms in bankruptcy court, because you could also think about what we were going to do with the FISA court in order to help expand that power that we'll be available to us to get a much better vector into when we understand – and then make it public like this.

So people realize, you know, we say there's two approaches. Either you want to hug the panda or you want to slay the dragon. Are you a dragon slayer or a panda hugger? Well, I think we really need to have our panda trainers and we need dragon trainers, because we have to get these major adversaries back on a sort of keel for us to go forward because if we don't get it right, my advice always for free is I encourage you to have your children learn Mandarin, which is what I'm doing with my grandchildren.

CINELLI: If I could make an observation, just two seconds, the Department of Defense publishes targeted U.S. technologies every year and they have done it for a long time. It has never included access to court proceedings as a way for targeting U.S. technologies.

RISHIKOF: I would say that we used to have the Economic Espionage Report.

CINELLI: Yes.

RISHIKOF: The last one came out in 2011.

CINELLI: Right.

RISHIKOF: That administration was not happy with the outcome.

CINELLI: Right.

RISHIKOF: And now the only entity that looks at it is usually coming out of the – what used to be called the DSS, the Defense Security Service. It's now the Defense Counterintelligence Security Agency. They published a very famous report that took over from when the report that NCIX made, but it's sort of sad that's where it's gotten now pushed to, and it's sort of sad when you said it's coming out of the NDAA, these are coming all out of departments, defense departments power as opposed to – other elements of the state.

CINELLI: Right. I mean, the Defense Production Act allows for a fair amount, but I think that the question that I just wanted, two seconds before Camille was that there are tools that are publicly available. These reports are incredibly insightful and helpful and even adding a small segment that says, "Look at it holistically." The government's looking at this as the whole of government. We need to look at it as the whole of society, as you said, and the whole of industry and including that kind of information about the access to our court system and the bankruptcy courts in particular would be very educational across the board.

RAVICH: I agree. Camille, quickly, before we turn to a Q&A?

STEWART: Yeah, I just wanted to take a moment to illustrate Giovanna's point on the complexity of identifying these national security related technologies, as well as to highlight the importance of technology to support judges in this endeavor, because it is so complex.

So recently, Grindr was sold to a Chinese company and that was rolled back about two years after that sale was made. Grindr is a dating app, so that capability would not on its face seem like a national security related sale, but the kind of information that can be collected, and when aggregated with the other information that is available about people –

JAFFER: And stolen.

STEWART: Well. Can social engineer you know, a great multitude of things and is a behavioral targeting mechanism that is just in a really advanced capability. Right?

But on its face, no one would have ever, particularly without some kind of training and support, been able to identify as something with national security implications.

So beyond also training judges, because to your point, the 27 NAICS codes are out of date in terms of like being forward-leaning on emerging capabilities and things like that, we need to figure out a technology solution that can take a look across economic development, innovation, and help flag these things for judges.

JAFFER: And can scale.

STEWART: And can scale. Right.

RAVICH: So on that point, before I turn to Q&A, we at TCIL, as you said we like to build and pilot solutions, and part of those solutions are not just in the education and helping to educate lawmakers, but in the technological side as well, so we are partnering with this alpha

data out of California, Caggle, that runs contests for different types of algorithms. We've given them a database to work from. What we want to achieve is exactly, as Camille is saying, a prototype of, if this is the information, the data that's already in the database of sensitive technologies, of things that have ITAR or E-A-R, that when a bankruptcy proceeding comes on a docket, it can be matched to a database of these are our existing sensitive technologies, and it can flash for the judge. Greenlight, fine, go ahead. Yellow, pause. Red, send it immediately for CFIUS for review, because one thing we realize, and when I talk to big companies about cybersecurity, companies have – that are just manufacturing something, are not cybersecurity companies, they always look at me and they're like, "But we're not cybersecurity experts. Do we have to now become cybersecurity experts?"

I'd say the same thing with the judges. Do they now need to be able to keep all of that in their head, the 27 NAICS codes? No, of course not. We need in part and parcel to the education, we need some kind of technology that can help match this with selectors to be able to give them the ability then to say, "Oh, I'd better call the guy at Treasury, take a look at this, so we are here at the lab, we're piloting a scalable version," and then giving it to the government or whatever to then take it to scale.

Okay. With that we have, I don't know, something like 20 minutes for Q and A. So, there are mics. Please wait for the mic and don't forget to introduce yourself.

SPEAKER: Hey, thanks for your work on this. The ATopTech bankruptcies and the Molycorp bankruptcies happen before FIRRMA and bankruptcy judges don't have the authority to tell any buyer of any asset that they don't have to go through any sort of regulatory process, whether they're buying a hospital or something with licenses. Does FIRRMA extinguish any of the concern about this because of the era that we're in with mandatory declarations?

CINELLI: So FIRRMA does not itself take any action that's going to be left for the regulations to dictate whether it extends and FIRRMA right now is drafted to apply primarily to the CFIUS process itself. So there is not a direct solution that is facing – that we can derive directly from FIRRMA and interestingly, although FIRRMA included expressly certain types of debt and bankruptcy proceedings as a covered transaction, for CFIUS actually believed it had that jurisdiction prior to FIRRMA and there were a number of cases as you mentioned ATop and Molycorp both preceded FIRRMA.

I think the other issue though, and it is a legislative impediment, there's a lot of laws and regulations out there that unfortunately silo the way systems – the U.S. Government can use information. So information collected in one context within the government is not automatically shareable either amongst agencies, amongst branches of governments or even within the same agency, and so there would have to be some additional refinement.

Now to Camille's point and love to hear your view, I think the regulations may address some of that. That would give the bankruptcy judges some additional leverage to say, "Perhaps as a matter of closing this transaction, please present us with these authorizations and approvals because that is an appropriate transfer of the asset". And in certain laws, just, I can't believe I'm going to say this in public, but the judges could be personally liable if they permit violations to

occur. And I can't imagine any attorney would ever say that to a judge in court. So, but fundamentally, if an executive branch agency wanted to make the point in a proceeding, they could raise that with the judge.

RISHIKOF: It's never been a career enhancing move on the lawyer's part in my experience –

CINELLI: No. Ergo, why I don't litigate.

RISHIKOF: The attorneys in the room? That'd be an interesting option.

CINELLI: No, you turn the name, you call the Department, right, yeah, exactly. So, yeah.

WOOD: I'm Doug Wood and I'm a TCIL advisor, and one of the things I've noted in the past is a slightly different area of law, but contract dispute is another area where foreigners might dispute the award of a contract and tie up the work in court. And it's not because they want the work, they're just trying to tie it up.

RISHIKOF: Yes. As you know, lot of lawyers in town have done extremely well under DFARS.

CINELLI: Yeah.

RISHIKOF: And litigating those issues. A lot of homes in Palm Beach have been paid for and –

JAFFER: I mean there's not a contract that is awarded by the DOD that goes on –

RISHIKOF: And I think that DFAR reform for a contract awarding, I think lot of us would think would be a very good thing. But there are a lot of verses that have derived a great deal of living, doing the contests.

HERNANDEZ: Hi, my name is Danielle Hernandez and I'm a legal fellow at the Department of Defense. So I heard you say that it's not necessarily necessary for judges or attorneys to understand the technology. Do all of you feel that way? That it's not necessary that attorneys actually understand the technology?

RAVICH: Well, I want to restate, it's not that it's not necessary, it's just there's so much you have to do ON any given day to –

HERNANDEZ: Certainly. Yes.

RAVICH: Also be an expert on quantum or to know that this is the way we had talked about it before that some of these filings you won't, unless you really read through it and understand it you it won't pop out. It won't be that the top category is quantum.

CINELLI: Right.

RISHIKOF: I think you have to sort of dis-aggravate the concept, right? Because if you go to the Northern District in California, that bench has gotten an extraordinary number of cases tied to technology. We also have a cohort issue, which is as the younger people get on the bench, they're more attuned as to what technology has been and whether they've lived with it.

Third, I think the FJC, the Federal Judicial Center, and DAO are doing a number of courses to help assist judges understand the underlying technology. It's something Aspen Institute used to do for years and is continuing to do it. I think the bench has recognized the desire, but when you get to the high court, it's only recently that we have had a number, if you look at the law clerks and where they've gone, you will see many of them have gone into the leading university technological groups vis-a-vis where our time with the justices on these issues.

So I think there's been a clear transformation going on. But I would say all the judges I know are very intrigued and interested in wanting to understand this in a more full way and get a more neutral understanding of what the technology is. And increasingly more and more cases, as you know are filling the dockets on this technological issue. Many people in the Valley are not happy with the way many of the cases are being unfolded, and one of them is this issue with how we understand antitrust law. How we understand the issue who we're competing with, and that's becoming a many – I've been in a number of groups who are interested in trying to help the judiciary and the legislature understand what may be required for us to be competitive going into the 21st century because many of our adversaries do not have the same antitrust problems that we're confronting.

JAFFER: Well, yeah, we're also –

CINELLI: So I – Oh, I'm sorry.

JAFFER: We're also sort of creating antitrust policies where none exist, right? We're going after companies because they're too, they've succeeded too effectively rather than engage in potentially anti-competitive behavior. But to your question, I think about the question whether lawyers or judges need to understand the technology. Absolutely they do. I don't think that's what Samantha was saying. I think that Samantha's point was it's, you need to give them capabilities that allow them to ingest the information that's out there a lot faster in a lot more capable way. Right. You can't expect them to be able to dig through the filings, identify the potential threats and figure it out on their own. If we can build a capability, a technological capability combined with education we can provide them, then they can have both the capability and a knowledge base.

But to your question about technology, we're spending a lot of time at NSI in partnership with people like TCIL, the ABA and the like, and with the support of our donors to guide and educate lawyers on technology. We held our, we held our first actually tech lawyer boot camp to teach lawyers about technology. Basically starting with how does my iPhone work, right, to sort of beginning the conversation about a quantum encryption at Steptoe just this past summer. We'll be educating a group of federal government lawyers here in the next year. We'll be rolling on a

similar program for judges. The, bankruptcy effort is one aspect of the start of that effort. But we'll be doing a larger cyber intelligence, national security law training for judges with the Law and Economics Center at George Mason.

So you're absolutely right. It's a critical issue. Nobody's saying lawyers just don't need to understand technology better. And the flip side is for our legislators, our policymakers, they need more technologists informing them. So under a grant from the Hewlett Foundation, we've selected a group of 25 technologists, data scientists, coders around the country where we're actually taking them and teach them how to talk policy, right. How to talk to policy makers. They'll be here next weekend being trained on how to develop policy proposals and how to put them in the hands of legislators and executive branch policy makers. So we're doing both sides of it. Train the lawyers how to talk technology, the judges how to understand technology, and the technologists how to talk to policymakers.

RISHIKOF: At which underscore, the Hewlett Foundation has been extraordinary.

RAVICH: Yes.

RISHIKOF: The Hewlett Foundation has been extraordinary and a number of people, Eli Sugarman.

JAFFER: Yeah.

RISHIKOF: That have helped spearhead this, funded this and should be commended for doing this.

JAFFER: Absolutely.

RAVICH: Absolutely.

CINELLI: So I just want to raise – because I have a slightly different perspective. I understand what Harvey and Jamil have said. I think that when you look at the courts, there's an obligation to be able to identify issues. You don't have to have a PhD in quantum physics to be able to understand what happened to Schrodinger's cat. I'd probably mispronouncing that name. Okay. But the point is that –

So and outside counsel or counsel in companies have obligations under their ethics requirements to be members of the bar that they have to have sufficient understanding of technology, not just how to search for terms and papers and things, but technology itself as they bring cases. Because under Rule 11 you're required when you submit complaints and other documentation, you must be able to certify basically to their accuracy. You cannot do that if you don't have sufficient access to resources that allow you to identify the issues and speak cogently and competently on them. Now. So from an issue identification perspective, I think would be incredibly helpful to arm judges and counsel with more of what Camille and others were talking about. What are the key pressure points? What are the choke points, what are the initial inquiries you need to make? And from there that's why judges get to ask the parties to brief them. There

should be an obligation, if the judge needs to understand some of quantum physics, then the parties have an obligation to explain that to the judge in terms that are understandable and relatable to the matters before the court.

WILE: Thank you very much for coming today and this is very interesting. We addressed –

RAVICH: Say who you are. Introduce yourself.

WILE: Sorry, my name is Benjamin Wile. We addressed the bankruptcy of U.S. companies, however, I think the threat might go, extend a little further where it's not the U.S. company that goes bankrupt, but it's mother company. If it's a subsidiary of a company outside of the U.S., let's say Russia and China right now are giving many loans to defaulting countries, Venezuela and African countries and many others around the world where then that company in the U.S. is held accountable against this loan that they can give back and then it's a backdoor that bypasses the law system here. My question is how we can deal with that in courts here in the U.S.?

RAVICH: Interesting question.

RISHIKOF: Ah, well my sense is you know, we're seeing a very clever strategy that the Chinese are using for lending their funds around the world and when there's default judgements in those countries, there's a reaction as to what the Chinese then extract in order for them to have the loan made good. That's a separate international bankruptcy set of issues. But I think how you educate the countries to understand, going and receiving that type of funding and what the possible consequences are. And when we talked about what is in those contracts, do they fully grasp what the consequences are for the remedies in the contracts in those countries is an international sort of educational phenomenon that I think increasingly some high profile cases that you alluded to, people are starting to look much more closely on what those lending documents look like.

RAVICH: Yeah, and I would just add that, you know, just as in the years after 9/11 a whole discipline of terrorist financing kind of grew up. We really are behind the eight ball on creating a like discipline of, I don't even know, international financial intelligence and analytics because this is really where we're going to have to understand how our economy and our wherewithal is being put in the cross hairs.

RISHIKOF: And your point, we're not alone. The United States cannot do this alone.

ROSE: Herb Rose. I guess I go back a few years. I started practicing before the CAFC was established and back then the CAFC was one of the few courts that was recognized as having, at least the judges, having some expertise with science and technology. Now I don't know whether it's changed very much since then. That was primarily because they handled a fair number of patent cases.

RISHIKOF: Right.

CINELLI: What's interesting because the predicate, the precursor to the court of, the U.S. Court of Appeals for the federal circuit and the court, right was the Court of Claims and you had judges that handled, let's say customs and international trade cases that may or may not have the had the expertise but for example, Judge Rich who was one of the original drafters of the 1952 patent law was on the court and had an encyclopedic knowledge of technology, and issues and he used to bring clerks that had similar background to it and an alternative solution is perhaps the court could have two or three clerks that are technologically sophisticated that are shared amongst the judges.

RISHIKOF: Well we have special masters that the courts can always establish –

CINELLI: Right.

RISHIKOF: But I think part of the issue is we – the way the federal system has evolved different jurisdictions get to become, because of the rate and volume of the cases, they start to become much more expertise on issues. Right now, the D.C. court of appeals and D.C. court trial judges are probably the leading authorities on terrorism issues related to Guantanamo. And related to –

JAFFER: You don't know anything about that.

RISHIKOF: No. I would say that whether one agrees or disagrees with the judge's opinions, they have an expertise and they've evolved because of the cases. We all know if you, if you've an SEC problem, you're going to go to New York.

But you know what I mean? So we've evolved and then the question is, you're saying what is the appetite for the federal judiciary to start to have a level of expertise among the bench? We've always – we've created it for tax courts, we've created for certain highly technical areas. And it's an interesting question you're posing, is there a point in time now that we should think in the federal judiciary given what's happening with this level of technology, of carving out a space for a special jurisdiction which we've done for bankruptcy for instance, which we've done for labor. Is this a time that we should have a public debate about it?

CINELLI: And I think one of the other things to consider is, because I agree with you Harvey, there are courts simply by the nature of the number of cases that are brought. You mentioned I think California –

RISHIKOF: Correct.

CINELLI: That the different district courts and the ninth circuit that have an enormous number of software cases. But I would make an observation, for example, from the protective orders side, the ninth circuit in the district courts in California are weak on protective orders related to export controls. They really, the language they have embedded in their standard protective orders that are used in every matter are not adequate to inform parties of their obligations, they're conclusory in nature. And they candidly don't assist the courts in

understanding where the different pressure points exist. So they've got years and years of experience but the effectiveness.

RISHIKOF: So Camille, you're next law review was just been put forward. About what the motto should be for the protective orders. How perfect. We look forward to reading your next educational scholarship.

CINELLI: Actually we are working –

STEWART: I was just going to say, we're already on that

RAVICH: Another, another question. I think we have time for one more. So, if not, I'm going to see whether the panelists, some kind of concluding comments that they would like to make. Yes.

CINELLI: You start Camille, go ahead.

JAFFER: Camille, this is all yours.

CINELLI: Go ahead, you start it and then we'll finish.

STEWART: Yeah, so I think we are in a good moment to make some progress on this. It is very clear by the expertise on this panel that there are smart people looking at the issue. We just need some mobilization of folks to take a look and to really put some money behind a lot of this. We've been having some interesting conversations on the Hill and like I said with Treasury that really has shown promise for progress in this area. But to the gentleman's point earlier, there's a lot of work to be done across the court system to make sure that our judges are equipped on these issues and have an understanding that rises to the level and is able to adapt and evolve with the changing times and the changing capabilities. So there's a lot of work to be done here.

CINELLI: Oh –

RISHIKOF: Go ahead.

CINELLI: I was, I think what... I think the issue is right now, the tomatoes have arrived, as to use Harvey's analogy and I think in part it's been driven by the extensive concern regarding the pervasiveness of this issue. Many years ago this was viewed candidly as a Department of Defense problem. It is now everyone's problem, the court system, every government agency, every company, because no one has no data, no one has no access to cyber and technology because it's just a matter of course to protect the information you have, and no one tends to work insurely in the United States. Everyone is global in some fashion.

So I think we have a perfect storm, a confluence of circumstances now where the issue is ready to be addressed and my only, my only hesitation is sometimes these types of time periods and inflection points push the responses to the extreme, that then need to come back. But I think we have a clear opportunity, not only in the research that Camille has laid out eloquently in her

article, but the work that's being looked at to bring a measured response that is both effective and able to withstand the long-term.

RISHIKOF: I would concur. When I was the Dean of the National War College, we always said that you look through our arc of history, there are certain core inflection points, and I think many of us agree we're at an inflection point now and I think if we dither and we let this moment go without going forward in a manner that we will, our grandchildren will look back to us and say, "Oh, they were the group –

CINELLI: Yes.

RISHIKOF: That figured out how to lose the special thing and precious thing we have". So we are forced to what you're saying, I think there's a consensus among certain groups and we at the ABA, you at FDD, you at the Scalia thing, the private sector. It's very, very critical that we work with our extraordinary power at DOJ to coordinate this in a manner that we can be proud of. So I would say, why don't we come back in two years and see whether or not we've been successful in doing this as a criteria that we could all gather and see how, what kind of score we give ourselves.

RAVICH: Great penultimate word.

JAFFER: Look, I'd say but for Camille's work and the work that TCIL has done on this issue, we wouldn't even know about this issue. So thank you for that work. Thank you for partnering with us. And like Harvey said we'll be back in two years and see how we did.

RAVICH: Well again, let me thank everyone for coming out for this critical issue and I've told a number of people this truly is, you know, in my career as long as it has been, maybe the first time where when we pose an issue, no one has said, "Oh, this isn't an issue, don't worry about it". Right. We didn't get any pushback on that. And when we didn't get any pushback of, "Don't worry, we've got it under control". Right. The typical response when you go to different agencies in the government. "Don't worry about it, we're doing it, if you only knew it we were doing it". No one said that. So we're really proud to have identified this and trying to close gaps. But again, thank you so much. They stay in touch, stay in tune, and keep in touch for what else we're, we're working on. So thanks.

RISHIKOF: Thank you.