

Episode 7- CFIUS Mitigation

Olga Torres: Thank you for joining us today. My name is Olga Torres and I'm the Founder and Managing Member of Torres Trade Law, a national security and international trade law firm. Today we're joined by Albert Schultz, the Founder of Kaerus Consulting, LLC, which provides mitigation services to companies under compliance agreements with the Committee on Foreign Investment in the United States. He started his career in national security and served 14 years in government, including five years overseas in Latin America. He continued to work as a government contractor for an additional 14 years, specializing in counter terrorism, counter proliferation, and telecommunications. During this time, Albert was also an infantry enlisted member, and infantry officer of the Army National Guard and Army Reserve.

He earned a degree in Economics with honors, from the University of Chicago and a master's degree in Management with distinction from the London Business School. Alfred, thank you so much for being here. We're excited to have you.

Albert Schultz: Thank you. This is my first podcast ever so I'm happy to do it with you.

Olga Torres: Well, we're still in our pilot series, as far as I know we say we're going to do five, we're going to see how we do and, and the feedback that we get. And so it's new for you, it's new for us as well.

Albert Schultz: Awesome.

Olga Torres: So today we're going to be discussing issues related to your work specifically before the Committee on Foreign Investment in the United States, we call it CFIUS. And CFIUS, for those of you who may not know what it is, it's an interagency committee and it's authorized to review certain foreign investment transactions, involving specifically foreign investment into the United States and certain real estate transactions as well. The idea is that they review to determine the effect of such transactions on the national security of the United States.

Now, for the most part, CFIUS filings are voluntary submissions by the parties in the transaction. In some instances, now, to new reforms of the law, we have mandatory filing requirements. Those can get triggered, for example, if the target company meaning the US company deals in certain critical technologies.

Something that comes to mind for example, would be if the target company is a defense contractor, they manufacture items control under the International Traffic in Arms Regulations the ITAR. So those would be situations where you get into a different category, you have a mandatory filing, but for the most part CFIUS it's still largely a voluntary filing regime, if you will.

Now we also know that CFIUS has a new team of people. And I say new, it's been a few years, reviewing for non-notified transactions, that's how they're known. So, if parties do not do a filing, CFIUS could still have the opportunity at a later time to learn of the transaction, learn that there was no filing. And in some cases, they could require a, a filing post-closing and in your worst-case scenario, they could even divest an acquisition. There's no statute of limitations for this review.

Now in connection with the CFIUS review, as advised by CFIUS, the president could actually suspend or prohibit any covered transaction when in the president's judgment, there's credible evidence to believe that the foreign person exercising control over a U.S. business might take action that threatens to impair the national security of the United States. Now, the good news is that this doesn't happen very often. We have seen more cases in the past few years. You may have heard things in the news, for example, typically involving adversarial governments, for example, let's think of China, and transactions that require a little more scrutiny, but for the most part, most CFIUS transactions get cleared in a subset of transactions. However, the clearance may come with conditions. And a lot of those conditions, for example, could be mitigation measures and it's going to be the focus of the podcast. What is mitigation? What is a mitigation agreement? How do they look? How do you deal with these measures? And that's when Albert is going to come in and give us more insight into his line of work.

And I guess Albert, we can get started with that, but before we do, if you can tell me more about your how your career started. I understand that you worked with the government, you worked, you worked abroad in Latin America for a period of years. How do you end up with CFIUS work?

Albert Schultz: I went to the University of Chicago and I ended up, not really knowing what to major in. So, I fell into economics just because the university is famous for that and it worked out well because I'd always been somewhat interested in international relations. And so, I was recruited to do economic analysis and I subsequently worked with several agencies at the Department of State, with the Department of Defense and other agencies. I did that for a total of 14 years and that included my five years of service and embassies in Latin

America. And then I decided to try out the private sector. I resigned and I went to London Business School and got this fantastic job in the City of London. That was really interesting work and, and they liked me so they said, promised me management track and equity and all this kind of good stuff. But it just happened to be right before September 11th happened. And so, like so many other people, I didn't want to be there just making money when, my country was under attack.

Olga Torres: Right.

Albert Schultz: I wanted to come back and help out. But at this point, both my wife and I had gotten our MBAs and so we had about \$200,000 in student debt back then. And, and she said, honey, I want to support you in this, but there's no way we're going to go back and live on a government salary. Just, it wouldn't work. So, I came back as a contractor and I did another 14 years as a contractor.

Olga Torres: And you were back in the States then?

Albert Schultz: Say that again?

Olga Torres: When you were working as a contractor, you were back in the States?

Albert Schultz: No, I was different... Yes, came back to the United States. I'm sorry, I missed that. So, I ended up starting my own company and this was a bit of good luck while I was in business school. One of our, one of my colleagues, another student from Germany, she sent a message out to everybody, an email saying, "Hey guys, we're going to graduate soon and we need some way to stay in touch with each other. And I found this really cool website that will help us do that." So I went to the website, it was called RYZ, R Y Z ryz.com and I didn't know it at the time, but it was one of the very first experiments in social networking. So, I go to the site and it's very confusing, I talk about profiles and connections and private messages stuff, which is all very familiar to us today. But as I started to understand it, I thought, wow, what a great tool for international relations, for national security, for public diplomacy, for example. So after I came back in as a contractor, I decided to do some experiments using these developing tools. And, in fact, I was think I was probably the first person in the whole national security establishment to be working on this.

Olga Torres: That's very interesting.

Albert Schultz: Yeah, so it was, some of the first briefings that I gave were, were hilarious. One of the most, prestigious, or I shouldn't say prestigious, the, one of the most distinguished individuals that I briefed, and probably the one of the most respected people in the Department of Defense. I got to my second slide and he put up his hand and he stopped me and he said, "Albert, thank you very much for coming in, but this isn't going to work." And I said, "What do you mean?" And he said, "Nobody's going to put their personal information on the internet for everybody to read. Why would they do that?" And I said, "Well, you're right. I mean, you wouldn't do what, I wouldn't do it, but there're people doing it." He said, "No, nobody's silly enough to put up like, where they are or what their families is or their, their kids' ages, or if they're traveling so people can break through their homes." And I said, "Look I know you don't believe me, give me the opportunity to try some experiments." He says, "Yeah go ahead and try, it'll never amount to anything." And the ironic thing about the story is that the next time I connected with him was 15 years later on LinkedIn, so he got my message.

Olga Torres: Well, on a side note, I think my first experience with social media was Myspace and it, it is kind of funny that you say it like that at a personal level. I've always wondered what happened to that profile, it just kind of disappeared. I don't know, I lost track of it and I'm like, it must be somewhere out there.

Albert Schultz: So this Myspace was actually, it probably doesn't exist anymore. Myspace was sold to a Malaysian.

Olga Torres: Thank God.

Albert Schultz: A Malaysia music company, it became a music platform. I believe that the profiles were just disappeared. But I'm talking even earlier that this is before Friendster, when I first started getting into this. So, I really was into it. Anyways, I started my own company to provide social media services for government agencies and it started to grow and eventually I sold it to another defense contractor.

And at that point I decided to retire. My goal at that point, my plan at that point was to just lie on the couch for the rest of my life and watch Netflix. My wife realized that wasn't going to work before I did, but then eventually I got bored. And about that time, I got a call from my investment banker that helped me sell my company. And he said Albert, "What are you doing nowadays? because I can't see you just lying on the couch, watching Netflix, the rest of your life." And I said, "Well, that's kind of what I'm trying to do, I'm exhausted." And he

said, “Well, do you have anything else in mind?” And I said, “Well, I thought about board service.” And he said, “Huh, let me give you a call back,” because he was in touch with a company that needed what’s called a Security Director for a CFIUS job. So that was my education about the world of CFIUS, of course, like most people I'd never heard of it before. And that's how I began, doing CFIUS work.

Olga Torres: And can you tell us more about, how does mitigation work with CFIUS or how do you get involved? If it, and we're not going to get into the technical aspects of the filings, but just for people to understand. Basically, like I mentioned before, we have filings that are submitted to this Committee, and they review the transaction. Typically, there's a foreign investor. They're acquiring a U.S. company, they review the transaction. In some cases, the government determines that there's a threat to national security. Can you give people an example of what would this mean? How would that look like? What would be a threat to national security and why does that lead to mitigation?

Albert Schultz: Absolutely, and I think the first thing to say is that the vast majority of filings do not result in, they're cleared right away. So, you're a German company, you want to buy a dog food manufacturer in Kentucky, nobody has a problem with that. And the policy of the United States is we love foreign investment, it helps everyone in the country, it helps our economy. In some cases, the proposed transaction is ridiculous on its face. We don't want to, a Russian company to buy the factory where we make missiles that we're shooting at Russians in Ukraine right now, or the Ukrainians are shooting. So that would be like no way, this is never going to happen. Why did you even think that we were going to approve this? In some cases, they want to let the transaction go through, but they have certain concerns.

So, the concerns typically fall into certain rough categories, this isn't by statute, but just what I've observed. One is intellectual property. We don't want to provide our adversaries with anything that is useful for our national security and might put us at a disadvantage. That's probably the biggest one. Another one is personally identifiable information about U.S. citizens. That's become increasingly important, particularly with the advent of artificial intelligence. So we want to keep that out of the hands of adversaries, that extends also to biometric data and medical data. One case I briefly worked on involved blood plasma, for example. Another broader category or what we call proximity issues. And this is where the investment would take place in an area geographic area, which is close to some sort of typically a military activity, military training, where the thought is that a foreign intelligence service would be able to collect information or data from the ongoing training, those are called proximity

issues. In those cases, you might see things that look like they don't have to involve national security, but they certainly do. The best example I can give of that, there was a Chinese company that wanted to buy the Coronado Hotel in San Diego, and that's close to right over where the SEALs train there, in Coronado beach. So, that was nixed.

Olga Torres: So, the government decides at that point, there's a potential threat to national security. We will approve the transaction subject to certain conditions, and then at that point we started looking into mitigation. How does that look like and what would be your specific role in a mitigation agreement?

Albert Schultz: An agreement is reached through negotiation by the parties. So, there's the target U.S. company, there's the foreign investor and the U.S. government and they negotiate, they identify...or, the government says "This is what we'd like to do and or where our concern is and how we can try to prevent, for example, IP from going back to China or prevent the Russians from building an installation right next to, I don't know, the Central Intelligence Agency or something like that. So, after that negotiation takes place, a document, there's a couple forms of them, but the one I've seen most often is called National Security Agreement or an NSA. And that specifies exactly all the mitigation steps. Those can take various forms. For example, they could be purely legal or corporate forms where there's a board declaration of some kind that we won't share certain information with the foreign buyer. That's less and less used as the government has decided to not only trust, but verify more.

So, other things that could happen is they could request the appointment of a security officer. They could request something called a third-party auditor who goes in and looks at, for example, the IT system of the acquired company and determines how vulnerable it is to have intellectual property sucked down. For ongoing manners or something called a third-party monitor, whose role is basically to ensure that all the mitigation and the National Security Agreement is adhered to also within the corporate structure of the acquired company. You can have a security director who actually sits on the board and has the full voting rights of any other director but has special responsibility to national security. And then finally and there's certain situations that require trustees or even proxy voters. Trustees I've typically seen when there has to be a divestment, as you referred to before. I was involved in one of those where, some Russian investors had managed to buy a part of a high-technology company with unique technology and when CFIUS found out about it, said, "No way, you have to sell those shares and we don't even trust you to sell them. So we're going to get Albert to be the trustee and he's going to sell the shares." And then, depending on the degree of risk, even an entire proxy board can be set up

for the U.S. company where they make all this business decisions at the board level and they only report financial information back to the acquirer.

I think what I'd like to emphasize is that in all these roles, the third-party monitor or the individual or the entity that's brought into monitor the agreement, their first priority, their first duty is to the national security of the United States. Only consistent with that first duty is their second duty is to promote the interests of the company and the company's wellbeing and financial wherewithal.

Olga Torres: Very interesting. We've been mentioning non-notified transactions and it was interesting that you mentioned, there was one where you were involved in it involved Russian ownership. Just for our audience and especially if they're not as familiar, sometimes the ownership structures in some of these deals are very obscure and it takes a lot of analysis to finally get to the bottom of the real ownership. And in some cases, it could be publicly traded companies. And so, some of the ownership is never going to be truly known to a certain extent because it's publicly traded. So that's what makes some of these very interesting in terms of assessing potential threats to national security because foreign actors, especially in certain jurisdiction, they understand that it would invite scrutiny by the U.S. government, so, in many cases it's not exposed and really easy to discern some of these ownership structures.

And in terms of non-notified and specifically for my practice, we do CFIUS work, as you know, and we are not a big law firm where we have a giant corporate practice feeding some other M&A work to us. So we come in typically, and a lot of the work that we do is on the analysis before any kind of filing. So we're getting contacted by law firms all over the country, that don't have CFIUS lawyers. They marry the export control analysis to determine critical technologies to the CFIUS mandatory assessment, for example. We get brought in and we assist with determining could there be any critical technologies. And oftentimes companies, especially in situations of startups, they're like, "We don't export our software, we don't have any exports to the U.S., we've never classified anything." So, it's a really interesting analysis. And in many cases, we don't have any critical technologies, we feel comfortable, there's no mandatory [filing]. But in some cases, hey we think it's prudent to have a voluntary [filing], depending on the parties and their appetite for risk, they may go for the voluntary filing, they may not. And so, in terms of non-notified, it's something that we have been emphasizing, especially if people say, "It's a voluntary filing, we're not going to go for it. We are in a, let's say we're in a friendly jurisdiction." I don't know, I'm making this up. "We're a UK based company. We are not acquiring anything too scary." In terms of non-notified,

do you have any sense, and I know that that there's some industry groups right now soliciting surveys to figure out what some of these non-notified transactions, what are they focusing on. Are there specific industries? You mentioned Russia, which would make sense. But are there any specific industries that, whether you're of counsel, corporate counsel or you're an investor and you're trying to, "Oh, do I file? Do I do the voluntary filing and live with the risk that CFIUS can always forever and ever come back and review the transaction? Or do we do a filing now that we have the short declaration, which is supposed to expedite things, do we do that?" Like, do you have any sense for the non-notified transactions and what the focus is?

Albert Schultz: Well, before I mention that, I don't think we've mentioned yet that once CFIUS clears a transaction, then the parties have safe harbor.

Olga Torres: Yes, safe harbor.

Albert Schultz: So that's a big reason to consider going forward with this. Just because you're from the UK doesn't mean that you are exempt from CFIUS action. Now, as an attorney, you know more than I do that there's a list of lower-risk countries that have been incorporated. But I have done mitigations on Canada, Canadian investment, and you can't get much more friendly and neighborly than that. The other thing to bear in mind is that CFIUS jurisdiction is very broad, and if there's any kind of interstate commerce that the U.S. target company does, that's enough of a hook for them to get jurisdiction and to examine it.

Olga Torres: That's a really good point. Again, for people that may not be as familiar, I think part of the analysis is determining, "Are we subject to CFIUS jurisdiction?" Because if you're not, you're good. And then once you determine that there is CFIUS jurisdiction, do you have a potential situation where you should consider a voluntary filing? Or do you have a mandatory. So, there's prongs to it and this is higher level than, we can get into the weeds in, in more of a webinar type format.

Have you seen any mitigation where it's so burdensome for the parties and going, talking about deals falling through that the parties just walk away? And part of mitigation it's tricky. Because every time we prepare for a filing, we typically have mitigation in the back of our head.

That's part of preparing in a good way to avoid potential mitigation. So, what's their cyber security like? How are they going to be able to restrict foreign persons from servers? What is their security access going? You always have

that in the back of your head as you're preparing some of these filings. But have you seen, in your experience, any deals that once they arrive they reach the mitigation stage and it's so burdensome that the company that acquired just says, "It just doesn't make sense for us," and there's no agreement between them and the government?

Albert Schultz: Yes, I have and, sometimes the government or one of the particular CFIUS monitoring agencies or CMA's, which are designated by the Committee to monitor a particular transaction. They do not feel like they have a good level of trust with the parties. And so, they will put in every bell and whistle into the national security agreement and make it quite expensive. So, I've seen a case where the Department of Defense really didn't seem to trust the parties and so they required everything. They required a third-party auditor, they required a third-party monitor, they required an internal security officer, they required a security director and so I was asked to bid to be a—

Olga Torres: That must have been a nice bid for you to submit.

Albert Schultz: Well, no. Be careful because I saw this and I think it was for the security officer role or third-party monitor, I can't remember what it was. I looked at this and I said, "Wow, this must be an extremely complex transaction and it'll take a lot of my time. I'll have to interact," there were actually two boards involved. I had to attend every board meeting, all this kind of stuff. And so, I upped my price on my bid, figuring this is going to take a lot of my resources and I sent it in and I get a call back from the attorney for the acquiring party. And she said, do you understand? There are only 12 people working at the U.S. firm.

Olga Torres: Wow. Yeah, it happens.

Albert Schultz: So, they just didn't want it to happen. The government, or in this case it was Department of Defense, and I'm not mentioning the names of any of the companies or anything, but it was clear that there was no trust there. And so, they overburdened it. And in this particular case, I don't have any knowledge of whether it went forward or not. I have heard of other cases where they've walked away, other ones where I've bid on it and I didn't get the work because they just decided the last minute not to go forward with the transaction because it was too burdensome.

Olga Torres: I've had the same experience. What about changes during mitigation? For example, in my experience during COVID, we were assisting a company with meetings with mitigation with DOD monitors. And COVID hits,

I think the year before we met in person and we sent someone from the office, and COVID hits and everything after has been calls. So, I think for the most part, you can still cover the same questions and express the same concerns and they still do the same type of review. But are, are you still seeing some of these be via teleconference? Are you expecting things to revert back to pre-COVID and do more in person?

Albert Schultz: In general, I've found the CMAs, the CFIUS monitoring agencies to be very reasonable. If you can elucidate or enunciate a business rationale, why maybe this doesn't make sense, then they'll certainly listen to you. And that's frankly where role where these third-party monitoring agencies or security directors and so forth can play a role because if there's not a hundred percent trust in the transaction parties, then in my role, I can almost mediate between the parties and the government. Just one quick example, there was an oil and gas case I was involved with. I reported that they had discovered a broken lock on one of the fenced areas to get into the oil pad where you see the little pump going up and down. The response from a Department of Defense was, "Oh my goodness, we have a tangible evidence of a break in. And so we require armed guards and roving dogs and 24-hour camera service" and the whole list of everything you could think of. And so at that point, I was in a position where I could call them up and say, look, this happens all the time in South Texas, and maybe some kids, or maybe a contractor was trying to go in to take water, put water on the site and they didn't have the combination and so they just broke the lock and got in. So the company's understanding that people in my position, our first duty is to national security. They can still look on us as a resource to explain business requirements to the government. Many of the folks that work in these roles on the government side have not been in the private sector and don't understand profit and loss statements and some of the real burdens that these mitigation steps can put on a company.

Olga Torres: Yeah, that's very interesting. Are you seeing any mitigation trends or anything?

Albert Schultz: Olga, I didn't answer your question. So yes, during the pandemic, the CMAs were not working out of their offices. They had very limited staffing. There was a lot of virtual work and in the conference we attended, we understand that that was changing and, in fact, we were told we'd be seeing more site visits as we come out of this. So that's going to turn around. There's going to be more face-to-face work. I'm sorry, go on for your question.

Olga Torres: No, well that answers the question. In terms of mitigation trends, are you noticing anything worth mentioning?

Albert Schultz: You asked about particular industries earlier and alternative energy, wind power, solar that has become more of attention from what I've seen.

Olga Torres: Have you heard of fusion energy?

Albert Schultz: I have not seen any fusion cases. I don't know if there are any commercial fusion at this point. I mean, it's a laboratory technology we're all interested in and hopeful that will work out. I think that the interest in alternative energy is twofold. Number one, there might be a proximity issue. A lot of these times these big solar plants are out in the desert or in the big plain somewhere, and they happen to be near an ICBM launch facility. But the other one is they touch our national grid and it's become, more and more part of the consciousness of the national security establishment that the electric grid is a vulnerability for our economy. So I've seen that.

The other thing that was mentioned at one of the conferences, not this last one we attended about an earlier one was soft power issues. And in this case, there was a Chinese company that wanted to buy a U.S. charter school. And I would've thought, "Well, what would that have to do with anything of having national security?" And that the thought there it might be used for propaganda purposes to subvert national will and so forth through education of young people. So that's something I've never seen before but it's a new area to watch.

Olga Torres: That's interesting. Any war stories to close it out and anything that you can share with us that is interesting and also informative at the same time.

Albert Schultz: Sure. I think the best war stories are the ones that teach you a lesson as well as just are entertaining. Let me tell you about Grindr. So Grindr is an online dating app, like Tinder, for those you who are familiar with Tinder. They came under CFIUS review because they had been purchased by a Chinese investor, a hundred percent purchased. Why would the us government care about that? And it goes to personally identifiable information. And in this case, it's particularly you there's some individuals that might be particularly vulnerable because if you haven't come out of the closet and you're still working in the Department of Defense or CIA or FBI, you might be vulnerable to blackmail. So, somebody had the presence of mind to realize this was a real vulnerability. So, I was asked to serve as a security director on the board of Grindr.

Olga Torres: Very interesting, I did not know that.

Albert Schultz: Yeah, it was a fascinating assignment. We did manage to sell the company to U.S. parties at the end of a year's process. But my story was about the first time I went to meet the company. So I went in and I met the CEO and the general counsel, and they had called a general staff meeting where everybody was going to join. And, they said, "Can you address the staff?" And I thought about it. I said, "Sure." But I didn't know what kind of reception I was going to get, because I'm being imposed on the company by the government and because my CV had been circulated around, people knew I had these links to national security and Department of Defense and they probably thought that I was sent there to spy on them.

So initially I felt that there was a resistance to my being there. And I was sitting there in the audience, and everybody was talking about financial results and so forth and so on. And finally, he said, okay, "We'd like to introduce our new director, Albert Schultz. Albert, would you like to come up and say a few words?" And as I was coming up, I could feel those eyes on my back.

Olga Torres: Who are you? You are a spy.

Albert Schultz: Yeah. Like who is this guy? Should we trust him and everything? And I had no idea what I was going to say. So, I got up to the front and I turned around and I said, "My name's Albert Schultz. I'm going to be the new director on the board, I have a special interest in security. So, my job is to protect our users." And I have to tell you at that point I got along great with everybody. There was nobody holding back resources. Anytime I needed something, folks were willing to collaborate.

Olga Torres: Please provide more background on your actual role, basically.

Albert Schultz: Well, what I learned from it is, , there's a lot of discussion in the security, cybersecurity community about changing a culture within an organization. And of course, folks like you and I think it about from a national security point of view. But the change does not have to be motivated by national security. It has to be motivated by something that's important to the culture, to the company itself. So in, in this case, without really thinking about it, I was able to identify a part of their culture, the profile of which could be raised, it would also resolve the national security concerns or at help mitigate the national security concerns. Which was my duty. But at the same time, we were doing it for a reason that everybody understood. We didn't want somebody in Jordan to be thrown off a building because their family discovered that they were working on Grindr.

Olga Torres: That's such an interesting story. Are you still a board member there or?

Albert Schultz: No, we sold the company successfully to a U.S. investor. And so my role there ended.

Olga Torres: Okay, well, thank you so much for joining us today and thanks so much to our listeners for tuning in. If you're tuning in and not watching the videos, please visit our website. We have CFIUS resources. If you are actually able to see our screen, we will throughout the podcast, we will define some of the terms. We'll also send you to the committee's website where you can find more resources and we typically add resources at the end and just throughout the conversation. Hopefully we can touch base again very soon. Albert, thank you again.

Albert Schultz: Thanks Olga, good to see you.