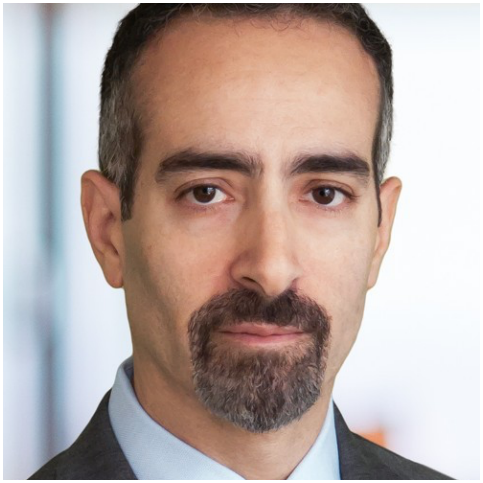
FEBRUARY 20, 2022

Former acting chief of DoJ's FIRS on lessons for dealing with CFIUS



This week, we sit down with David Plotinsky, who most recently served as acting chief, and principal deputy chief, of the Foreign Investment Review Section in the Department of Justice's National Security Division. Formerly the chief of the FCC's Cybersecurity and Communications Reliability Division, Plotinsky recently joined the Washington, D.C. office of Morgan Lewis. A 25-year veteran of government service, Plotinsky has also served as associate deputy general counsel for the Office of the Director of National Intelligence, where he was head of litigation for the agency; counsel for the National Counterintelligence and Security Center; counsel for the National Counterterrorism Center; attorney advisor in the DoJ's Office of Intelligence; and assistant counsel in the U.S. House of Representatives' Office of General Counsel.

Welcome David. Let's start with the recent move. What prompted the jump to Morgan Lewis?

One of the major considerations for me was that in my time leading DoJ's Foreign Investment Review Section, we worked on some of the most difficult cases out there, in terms of risk to national security, emerging tech, legal issues, and so on. In moving to the private sector, I wanted to be able to continue working on the most complex and novel transactions, and Morgan Lewis is equipped to do that type of work. The firm has a very deep bench, not just in national security but across the spectrum of other legal practices, which was important to me because the big cases in this space require a multi-disciplinary approach, so you need a diverse team that is able to handle all aspects of a transaction.

We're big fans of Giovanna Cinelli at Morgan Lewis, who made our "Top Advisors" list for the last two years. You going to be working with her?

Absolutely. (And I'm a big fan as well!) Although I certainly come to Morgan Lewis with plenty of experience based on almost 25 years in government, I also lean heavily on my partners who have their own unique backgrounds and can help get me smarter in any area where I've got a gap. So far, I've learned something

new every day since starting at Morgan Lewis, thanks to Giovanna and the many others like her at the firm who have tremendous experience counseling clients on a broad range of sensitive and high-stakes matters.

Okay, let's talk about the Foreign Investment Review Section at the DoJ, which I think is kind of a "black box" for most of our readers. Give us the lay of the land.

When I started at the Department of Justice in 2008 (in a different office), FIRS was about five attorneys, and the work the office did was important but generally low-profile. Fast-forward to today, when foreign investment review is top of mind for policymakers and industry, and FIRS is almost fifty people altogether, and the work it does is closely tracked by senior DoJ leadership, including the Office of the Attorney General and the Deputy Attorney General.

As the acting chief and the principal deputy chief, I had three deputy chiefs who helped me run the office — one for the CFIUS portfolio, one for the Team Telecom portfolio, and one for the Compliance and Enforcement portfolio — and also a Principal Scientific Officer who leads a team of technologists who work hand-in-hand with the attorneys. When I was doing a flood of hiring to beef up the office, in addition to the normal things DoJ looks for such as high levels of analytic and advocacy skills, I also placed a premium on people who were entrepreneurial, because this is such a dynamic mission space, and to some extent FIRS is writing the playbook at the same time it's in the middle of playing the game. That's probably not the comfort zone for all attorneys out there, but in FIRS that's where we thrived. I also looked for attorneys who had the skill set to work in an interagency environment — again, not everyone's cup of tea, but to work on national-level issues the way FIRS does, you can't act unilaterally, but rather you need to be good at navigating the interagency and the White House processes.

The final thing that is helpful to understand about FIRS is that it's the only office that handles both policy work and legal work in the same shop. Every other agency strictly bifurcates those two functions between an office of general counsel for the legal piece, and a policy office to actually do the mission; but in FIRS, all of the attorneys wear both the lawyer hat and the policy hat, and therefore have complete visibility and involvement across the full range of CFIUS, Team Telecom, and other work.

And the core function of FIRS is the evaluation of foreign investment in the U.S., yes?

Bingo. That being said, however, while I was at FIRS, the office was increasingly getting pulled into work outside its core mission, simply because it had the right expertise — and that's related to what I said earlier about the office needing to be entrepreneurial. For example, it was FIRS that led the development of Executive Order 13873, which gave the Secretary of Commerce new authorities to regulate supply chain security for U.S. information and communications technology and services. I was actually the initial drafter of that E.O., and although it doesn't really involve what most people would call foreign investment in the U.S., we did it because we identified an authorities gap where certain high-risk transactions weren't subject to either CFIUS or Team Telecom jurisdiction.

So, exactly how does FIRS interact with CFIUS. Is this like a daily process? Weekly?

Daily. Hourly. Minute-by-

minute. Without going into specific numbers, I'll just note that DoJ is one of the primary players in CFIUS. FIRS therefore co-leads a big chunk of the total CFIUS case load, and often some of the most interesting and challenging cases. And again without going into specifics, FIRS also is among the most active CFIUS agencies with respect to compliance monitoring and enforcement. A lot of the DoJ equities in the CFIUS process stem from DoJ's counterintelligence and law enforcement missions, and cases involving risk to sensitive personal data – which is a growing part of the CFIUS docket – squarely implicate DoJ's counterintelligence equities.

Let's dig into the topic of "monitoring and enforcement" you just mentioned, which we've covered extensively. Can you tell us a bit more about how FIRS gets involved in ongoing compliance monitoring with respect to mitigation agreements?

I'd characterize FIRS as taking a leading role in a lot of the CFIUS compliance monitoring work, and any resulting enforcement actions. In addition to the general explosion in the size of the office, one of our big organizational changes a few years ago was to establish a dedicated Compliance and Enforcement team, with its own deputy chief at the helm. Previously, compliance work was done by the same attorneys handling active cases, and we wanted to devote specific resources to compliance work so that it didn't become an afterthought. And in my mind, part of the reason compliance is so important is that it's really what enables the government to clear transactions. I think as the government you would need to block more transactions if you couldn't depend on an effective compliance system to mitigate national security risk, so in that way a robust compliance regime helps maintain the U.S. open investment climate.

Curious if there are any common pitfalls to avoid, or mistakes that companies consistently make, when dealing with CFIUS?

A lot comes to mind, but I'll mention just a few. First — and you'd think this would be obvious but there are companies I've seen that have problems doing this — you really need to be forthcoming in responding to CFIUS or Team Telecom requests for information. FIRS is full of very talented lawyers who are committed to the mission, and I promise you they're going to get the information they need — so if they can get it quickly and without having to pull teeth, the case will go a lot faster and more smoothly. Another potential danger area is signing on to mitigation measures without fully understanding the commitment involved going forward. For example — and I've seen this very thing happen — if you agree to limit access to certain data, but you don't have a solid handle on everywhere that data resides in your enterprise and how access is governed, there's high compliance risk of inadvertently mishandling that data and winding up with enforcement issues.

Any other final lessons you'd impart to others regarding CFIUS or the foreign investment regime?

One thing that may be under-appreciated is that CFIUS and Team Telecom cases overwhelmingly turn more on policy issues than legal issues. Legal issues — for example, ones surrounding jurisdiction and extraterritoriality — are important threshold questions, and definitely require careful analysis, but it's usually the policy calls that consume most of the government's attention. I feel like 99 percent of the time when I'd be discussing a CFIUS or Team Telecom case with senior DoJ leadership, the conversation

centered around policy decisions and risk tolerance, rather than fine points of law. So, for companies and lawyers out there doing CFIUS work, I'd recommend devoting significant energy to trying to think the way the government does, and looking at your transaction through the lens of how agencies — including their political leadership — currently view national security risk.

Great insights. Thanks David.

David Plotinsky is a partner in the Washington, D.C., office of Morgan Lewis. He can be reached at david.plotinsky@morganlewis.com or (202) 739-5742.