THE UNITED STATES DEPARTMENT of JUSTICE
STICE NEWS

Deputy Attorney General Lisa O. Monaco and Assistant Attorney General Kenneth A. Polite Jr. Deliver Opening Remarks at the Criminal Division's Cybersecurity Roundtable on 'The Evolving Cyber Threat Landscape'

Washington, DC ~ Wednesday, October 20, 2021

Assistant Attorney General Kenneth A. Polite Jr.

Remarks as Delivered

Good afternoon. We gather together today for our fifth Criminal Division Cybersecurity Roundtable, and the need for our collective action against cyber threats has never been greater.

Cyber threats loom over nearly every aspect of our personal and professional lives.

As a former United States Attorney, chief compliance officer and law firm partner, and most importantly as a parent, I recognize the critical need for public and private collaboration in addressing the enormity of the cyber threat.

Cybercrime is one of the defining issues of our time, and this afternoon we will discuss how government and private industry can best work together to implement an agile and robust cybersecurity response.

I thank our esteemed audience members for their participation today.

In particular, I thank my friend Matt Olsen, our nominee to be Assistant Attorney General for the National Security Division, for joining us today.

But first, it is my honor to introduce the Deputy Attorney General of the United States to open today's roundtable.

Having served as the Assistant Attorney General for the National Security Division and the Homeland Security and Counterterrorism Advisor to the President, Deputy Attorney General Monaco is a preeminent expert on cyber threats, and her considerable knowledge will no doubt inform the department's cybersecurity responses moving forward.

Ladies and gentlemen, the Deputy Attorney General of the United States.

Deputy Attorney General Lisa O. Monaco

Remarks as Delivered

Thanks so much, Kenneth. It's great to join so many of you from across the private sector today. Also, I want to echo, Kenneth, your welcome to Matt Olsen. We are looking very much forward to getting him here, back in the department and in the seat as the Assistant Attorney General for National Security. Again, thank you so much for letting me spend some time with you this afternoon. We in government know that we can't tackle the host of cyber threats we are facing alone. We cannot do it alone. Consistent engagement is key to our collective successes, so I thank you for coming today, joining this roundtable meeting and for sharing your perspective with us on how our partnership, an essential partnership in my view, is working.

I want to start today by taking just a few minutes to talk about how I see the current cyber threat landscape – and make a few observations on how I see it now, compared to when I was last in government. The bottom line is this – I think we're at yet another inflection point in terms of the types of cyber threats that our nation faces.

In my last role in government, I served, as Kenneth noted, as the Homeland Security Advisor to the President, and I had responsibility for coordinating cybersecurity issues across the government and our responses to a number of cyber threats incidents. At the time, the focus was most acutely on nation states actors – and I spent a lot of time meeting every morning in the President's daily brief, in that first meeting of the day with the President and the Director of National Intelligence and a number of other folks on the national security team, talking through the biggest threats, the most urgent threats, facing us every day. And I found that during that session over time, over the four years that I served as Homeland Security Advisor, an increasing amount of that meeting, of the President's daily brief meeting, was taken up by my briefing the President on nation-state cyber threats. On their destructive attacks, on their engagement in what I have come to call geopolitical one-ups-man-ship.

Now that threat remains today. We know that nation states, specifically the big four – Russia, China, North Korea and Iran – pose a significant threat to our national security, our economic security and our personal security.

And it's continued to be the case. We know that from Russia's engagement in supply chain attacks in the Solar Winds attack; by China's engagement in the Microsoft Exchange vulnerability exploitation and going after our own infectious disease research in the wake of COVID-19, just to name a few examples.

Now that I'm back in government – nearly six months to the day in this job as Deputy Attorney General – a few things have struck me: first, the overall environment is more aggressive; more sophisticated; and more belligerent in terms of what the actors are doing. The second thing that struck me is just the pure nature of the threat itself.

It's not just state-sponsored attackers, but now the threat is blended with criminal groups. They are forming alliances of convenience, alliances of opportunity and sometimes alliances by design with nation-state actors. Countries such as Russia and China are allowing this criminal activity to persist without consequence — if not expressly condoning such activity, they're acting as a safe harbor for these cybercriminals and turning a blind eye in often cases.

Meanwhile, these malicious cyber actors are attacking the critical infrastructure sectors here in the United States – our pipelines, our food supply, our hospitals and our first responders. So, the criminal groups and the threats that they pose, now have a national security overlay, they have clear national security implications.

The other thing that has struck me is the sheer brazenness of this activity. There is a brazenness to the tactics and the techniques being used, especially when it comes to ransomware and digital extortion.

When we think about the types of ransomware attacks that we've seen, and the impact that they have on critical infrastructure, with potentially life and death implications, the consequences of this criminal activity is, I think, designed in often cases to be quite severe.

So the last thing I'd say is I'm struck by just how broad this is. Just to illustrate this issue in the ransomware context, we know that the FBI is investigating more than 100 ransomware variants, and those variants are impacting thousands of victims. Suffice it to say, there is much to be done in this space, and to combat this crowded and aggressive threat landscape.

And so, we need your help. What are we doing here at the Department of Justice to address cyber threats?

One of my prior roles in the department is leading the National Security Division. I focused on applying lessons we learned from the counterterrorism fight and applying it to the cyber threat fight, making our approach more intelligence-led, more threat-driven, breaking down the walls between intelligence about cyber attacks and cyber threat actors and the efforts to disrupt them. And our focus on nation states and their destructive attacks, their IP theft – and we created the first nationwide network of national security cyber prosecutors around the country.

Today, the Department of Justice is a leader in the whole-of-government efforts that we have to keep our country safe from the cyber threats I've described, and our prosecutors around the country – national security focused and criminal focused – are working together to address this threat landscape.

We have never hesitated to evolve to meet the challenge that the cyber threat poses, and that mindset is exactly what's guiding us today.

Today, one of the top priorities the Attorney General and I have is to make sure that we are best positioned and situated to deal with the cyber threat, as it rapidly evolves. And consistent with this goal, one of the first steps I took when I returned to the department was to launch a Comprehensive Cyber Review, to make sure we are adjusting here at the Department of Justice to the speed of the threat in terms of what we are doing, and what tools we are bringing to the table.

So, this Comprehensive Cyber Review is designed to do three things. The first is assess how we can improve our capability to investigate, to prosecute and disrupt these actors and their evolving techniques. The second is we need to focus on building our own resiliency as a department, as a multinational, global organization when it comes to cybersecurity. And we need to make sure we're doing what we can do to prepare the next generation when it comes to the department's attorneys and agents to go after these threat actors.

We are not waiting to take action. We've already announced a number of initiatives designed to make sure the department continues to meet this set of cyber challenges. I want to highlight a few of those for you today – that I expect will be on your minds and should be on the minds of many of you and your clients.

I want to be clear. Today, I've got some very direct asks. First, in this threat environment, with the stakes that are involved, we cannot do this alone, so we need your engagement. And we want to hear from you. What are the impediments you are hearing from clients about coming forward and working with law enforcement, working more with us? The nature of the threat, the stakes that are involved, in my mind make it critical that we have that engagement – and nowhere is this more true than in the context of ransomware attacks.

Not a day goes by without ransomware headlines screaming at us from the newspapers. Earlier this year, the Department of Justice launched the Ransomware and Digital Extortion Task Force, to address this particular manifestation of the cyber threat.

Through this Task Force, we are making sure that the components of the department — including the Criminal Division, the U.S. Attorney's Offices, the FBI and the National Security Division — are all working together, bringing all of its tools to bear on this threat to ensure that we disrupt, investigate and prosecute not only ransomware groups, but also the entire criminal ecosystem that allows it to flourish.

We sent a directive to all 93 U.S. Attorney's Offices to say: where you see a ransomware event in your district, in your location, whether it involves a ransomware attack on a company, whether it involves a part of the ecosystem that allows it to flourish — we want to know about it so we have a national picture. It is the kind of reporting that we have required from the field for years after 9/11 when it comes to terrorist activity. We want to do the same heightened level of awareness and national picture reporting when it comes to ransomware. It's that important.

We are laser focused on investigating these cases and holding all those who help facilitate these crimes accountable — including, as I said, not only the attackers and the hackers and the affiliates who create and spread ransomware, but also the money launderers and the cryptocurrency companies that make it profitable.

Relatedly, I announced last week a new National Cryptocurrency Enforcement Team that is housed in the Criminal Division, drawing on its expertise, and I'm sure you will hear more about that later on in today's program.

We've made great strides in combating the misuse of cryptocurrency platforms. And we've shown we won't hesitate to go after those platforms that help criminals launder or hide their criminal proceeds. We did so this past August, when we secured a guilty plea of the criminal behind Helix, the Darknet Bitcoin mixer responsible for laundering over $300 million in funds for criminals.

But we want to strengthen our capacity to dismantle the financial ecosystem that enables these criminal actors to flourish, and, quite frankly, to profit from what they're doing. And we're going to do that by drawing on our cryptocurrency experts, our cyber prosecutors, our money laundering expertise across the department and centralizing and building on the expertise that we already have.

And when it comes to tackling the issue of ransomware and the ecosystem that lets it flourish — I want to be clear on a single message here: we need reporting from victims to address this threat, to prevent additional victims. We know those victims — oftentimes your clients — face reputational risks, they face operational risks, ultimately though, we are

seeing lives and livelihoods risked. Given the stakes, we need that engagement from victim companies and we need it early.

Those who come forward will see that we are determined to bring our authorities to bear, to be nimble in our response, to employ tools that go after the ecosystem that lets these bad actors flourish.

With the help of cooperative victims – we went after the money paid in ransom, we seized the wallet; we returned money to the victim in the Colonial Pipeline ransomware attack. We will go after the keys involved in these attacks and provide them to victims, without those victims having to pay ransom when we can. But we need your help.

So when you are in discussions with your clients and they ask: why should we go to law enforcement? Where are the benefits? Well, here are the benefits: we make arrests; we hold people to account; we get money back; we will go after keys and get them to the victim; and victims can help avoid liability through working with law enforcement and those companies that stand with us and work with us will see that we stand with them in the aftermath of an incident.

The bottom line is this: I believe it is bad for companies, bad for America, and it hurts our efforts to uphold the values that we try to demonstrate as a country, if companies are attacked and don't partner with law enforcement, and thereby help disrupt these activities and prevent future victims.

So we want and need your input, we need to make sure the benefits of coming forward and working with law enforcement are viewed as a positive – and on the flipside we need to make sure that there is tough enforcement where it's appropriate.

If companies don't come forward — in this threat environment, with the stakes being as high as they are in many cases – I think legitimate questions will be and should be asked of companies – why didn't you come forward and help prevent the next victim? That's why I've called publicly for a national incident reporting standard, because we can't go at this alone.

Another area where we're trying to bring all our tools to bear is on the civil side. We launched last week also a Civil Cyber-Fraud Initiative. And this is first time using our civil enforcement tools to drive cybersecurity accountability.

Now this is, I hope, particularly resonant for those with contracts with the government. We recognize that most entities and individuals who do business with the government abide by their contract terms and their obligations, and that cyber intrusions may still result even when a contractor has a robust monitoring, detection and reporting system. And we take very seriously our mission to help victims of cyber intrusions, and to encourage them to come forward promptly and work with law enforcement to remediate vulnerabilities and help in our effort to limit resulting harm to them, and to other victims.

But where those who are entrusted with government dollars – who are trusted to work on sensitive government systems – where they fail to follow required cybersecurity standards, or misrepresent their cybersecurity practices or capabilities, we're going to go after that behavior. Specifically, our new Civil Cyber-Fraud Initiative will use the False Claims Act to both enforce civil fines on government contractors and grant recipients as well as protect whistleblowers who bring information forward.

This is a tool that we have to ensure that taxpayer dollars are used appropriately, and to guard the public fisc and the public trust. And we will use it. And to those who witness irresponsibility that exposes the government to cyber breaches, our message is this: if you see something, say something. We will use all of the legal authorities in our reach to make sure you are protected and compensated.

Now, we at the Department of Justice know that some of our greatest progress and accomplishments to date in this area — both in the understanding of the evolving threat, and the disruption and dismantlement — could not have been achieved without a whole-of-society approach, which includes, most importantly I think, the close cooperation and work with the private sector.

We know we need to continue to innovate and work collaboratively and cooperatively with our partners and the private sector if we are going to keep pace with the challenges we are facing in this arena.

That means we don’t just want to hear from you — we need to. We need to hear about the challenges you face and the ways you think the department can evolve to help meet the threat. We need to hear what you think is working well, and more importantly, what you’d like for us to consider doing differently. So I really hope you use this event and this time as an opportunity to provide your views, your perspective — because we are ready to listen to them.

I know that the Assistant Attorney General Kenneth Polite and the Criminal Division have a great program planned for you for the rest of the afternoon, and I want to thank them and you for letting me spend some time with you today, and thank you for participating and providing your perspective.

Speaker:
Lisa O. Monaco, Deputy Attorney General

Topic(s):
Cyber Crime

Component(s):
Criminal Division
Office of the Deputy Attorney General

Updated October 20, 2021