wiley

Cyber Spotlight: Wiley Tackles White House's National Cybersecurity Strategy and Other Developments

Wiley Connect
March 17, 2023

Wiley Connected · Cyber Spotlight: Wiley Tackles White House's National Cybersecurity Strategy and Other Developments

In this episode of Wiley Connected, the cyber team discusses major changes in federal cyber expectations for the private sector, including the National Cybersecurity Strategy and new rules being created by the Department of Homeland Security. Join Megan Brown, leader of Wiley's Cybersecurity team; Lyn Brown, special counsel and formerly at the FBI; Kat Scott, partner; and Tyler Bridegan, associate, as they discuss what is happening, what comes next, and how to prepare.

Transcript

Tyler Bridegan

Hey, everybody and thank you for tuning in. My name is Tyler Bridegan, and I am the host of today's cyber spotlight on Wiley Connected. This episode is focusing on some big changes underway on cyber security. Last week, we saw the release of a new national cyber security strategy and there are many other major developments. I'm joined by some amazing cyber practitioners from Wiley Rein. First up joining us is Megan Brown who has been on the front lines of crafting and responding to nearly every federal privacy initiative since 2010. I'm also joined by Lyn Brown who, prior to joining Wiley as a national security and cyber security, experience at the FBI,

Related Professionals

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jacqueline F. "Lyn" Brown
Of Counsel
202.719.4114
jfbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

CIA, and the White House. And lastly Kat Scott is joining us, who advises on an array of clients from nearly every sector on current and forthcoming privacy and cyber security obligations. Welcome, everybody!

Megan Brown

Hi there.

Kat Scott

Hi, Tyler.

Lyn Brown

Hey.

Tyler Bridegan

So, thank you all for making the time. Last year, as we've covered in prior episodes, we saw a continued rise in the number of omnibus state privacy laws and the different obligations those impose on companies around the country. Fresh off those significant shifts in the privacy landscape, we're now seeing a similar seismic shift in cybersecurity at the federal level. It seems each week a federal agency is announcing a new cybersecurity rulemaking. So, let's start broad. Megan, how do you think clients should be approaching their cyber security strategy?

Megan Brown

Well, that's a great question. They're certainly dealing with a lot of incoming developments that are really challenging to keep track of. So, sort of basics is making sure they're identifying and sticking to best practices. Trying their best to stay ahead of new developments in any of the regulatory agencies that may touch on them. As well as at the department of homeland security, they've put out some cyber security performance goals that we expect to make into regulation at some point. We think looking at doing tabletop exercises, practicing your basic cyber hygiene. And maybe looking at some of the security directives and other things that are applying to different industries because you can get a sense from those where the government is headed for the broader private sector. Like just last week I think, in response to the strategy EPA has taken action on the water sector and TSA took more action on aviation. So, you know those are places to look and it is rapidly accelerating.

Lyn Brown

I think the key is preparation. Companies should have a cyber incident response plan and regularly schedule tabletop exercises to help them prepare for a cyber-attack. Especially a ransomware attack which can potentially cripple operations for a period of time. So not only have a plan, but have the relevant vendors lined up in advance like a forensic consultant, a ransomware negotiator, a payment facilitator, or a communications firm in order to save time at the front end of a cyber-attack. And track the government cyber

alerts to try to stay ahead of threats. And train your personnel on how to respond to or prevent a cyber-attack. Phishing remains one of the most prevalent means for threat actors to infiltrate company systems. Spoof emails, alter payment information. So, teach employees how to be alert to possible phishing attacks. And confirm changes in payment information in person.

Tyler Bridegan

So, it seems like, in addition to being prepared, there's been a lot of new cyber security regulatory activity coming out of Washington, D.C. Kat, what initiatives have you been watching closely?

Kat Scott

There really are just a ton. I mean we're involved in dozens of proceedings. I'll just name a few. DHS has to implement the Cyber Security Incident Reporting for Critical Infrastructure Act or CSIRCIA. That was enacted in 2022 and it sets in motion massive new regulatory framework and regime for private companies to report cyber incidents and ransomware events. Then you have the Securities and Exchange Commission. They have a pending rulemaking right now to require public disclosure of material cyber incidents for regulated public companies, among other things. The Federal Communications Commission has been really active in the cybersecurity space. They are right now proposing to expand their breach reporting requirements substantially. And that applies to CPNI. Then you have the Federal Trade Commission. The Federal Trade Commission has a lot going on. One of the biggest things happening right now is their data security and privacy rulemaking. And that is currently underway. You have TSA and the EPA. They have new mandates, some through security directives and some through rules. And then just dozens of work streams at NIST and DHS under several executive orders. They're looking at software security mandates, security labeling for IoT and connected devices, Megan mentioned this earlier, but DHS is doing cyber security performance goals for critical infrastructure and the list really just goes on.

Tyler Bridegan

So, the agencies have been busy is what you're telling us.

Kat Scott

Very busy.

Tyler Bridegan

So, in addition to that, last week the long-awaited national security cyber security strategy was released by the Biden administration and has been getting, for good reason, a lot of attention. What can you tell us about it?

Kat Scott

Yeah, well the strategy has 5 Pillars. They focus on groupings of cyber risks and responses. I think we're going to do a deeper dive later on in the podcast but, overall, it focuses on securing critical infrastructure, making it harder for the bad guys, investing in security and technology, allocating liabilities, and continuing U.S. cyber work internationally.

Megan Brown

And one of the key takeaways is that government oversight is going to substantially increase. The administration is moving away from using federal guidance as models. And instead, is moving to promote sort of baseline cyber security regulatory standards, some of which are pretty onerous.

Lyn Brown

Yes, I think the overall message of the new cyber security strategy is clear. The Biden Administration believes that the U.S. can no longer rely on voluntary collaboration and vigilance against cyber threats. So, the administration feels it must shift responsibility to industry through regulations, because it thinks the market has failed to incentivize cyber security sufficiently. We're moving essentially from the voluntary public private partnership model to a much more rigid regulatory regime.

Tyler Bridegan

That seems like a pretty substantial shift in sort of the regulatory frameworks that have traditionally been applied. Are there any aspects of the national cybersecure Cyber strategy that you think companies should be particularly concerned about?

Megan Brown

Yeah, I mean just to drill down a bit, the White House has made it clear there are more regulations coming, there have been regulations coming, you know, coming online for the past couple of years on a sector-by-sector basis and we're just going to see that accelerate. Um, just this week we saw 2 new moves. And there are you know, forthcoming obligations tucked into the strategy for internet providers. There's going to be several calls for legislation, a lot in the strategy is ambitious and needs Congress to act. And, quite frankly, I think the discussion of liabilities is risky because I think it has a risk of harming collaboration in cyber events. When you start encouraging people to point fingers at each other and think about liability and sort of damages.

Kat Scott

Yeah, I think that's exactly right. The other thing I'm a little concerned about is just this issue of conflicting and overlapping requirements. And what's not clear from this strategy is how the regulations that are going to be forthcoming and that are already here will be deconflicted, right? There are options to do it. This could happen through interagency process led by National Security Council or through the statutory mandates of the Office of the National Cyber Director. It could happen through the Cyber Incident Reporting Council that was established by Congress. And there's also an interagency group that's chaired by the FCC Chairwoman. But,

despite all these channels, we really haven't seen tangible movement toward deconfliction.

Lyn Brown

And I worry that some of these new mandates and calls for regulation, accountability, and punishment may actually make companies less willing to work, for instance, with the FBI which has made such inroads in encouraging voluntary cooperation in the face of a cyber-attack. That trust was not easy to build. And I would like to have seen the administration work to safeguard it and try and enhance cooperation with law enforcement more.

Tyler Bridegan

So, I noticed this strategy talks a lot about quote rebalancing responsibility. Can you just give our listeners sort of a preview of what that means.

Lyn Brown

Well, the White House is portraying the strategy as a rebalancing of responsibility, so that risk is not devolved down to small businesses or individuals or local governments. The theory is that the most capable actors, including the federal government, should do more. And think it's important to note that the most capable actor's language seems particularly focused on Cloud providers and software or hardware manufacturers.

Megan Brown

And I think this is where the strategy where things get a little hard from a policy perspective and a legal perspective. The administration is suggesting, and this was true with the rollout as well, that consumers and users and localities are basically unprotected and left to fight nation states by themselves. It's not really exactly right. I mean yes, there are disparities in resourcing and capabilities, but companies and service providers do a ton presently to defeat cyber-attacks. And there are a lot of things that small and medium sized businesses can and should be doing and are doing, quite frankly. And from my perspective, the government, instead of sort of trying to reallocate or create liabilities and responsibilities, should be looking to help the private sector. Both helping the smaller folks, and people at NIST have asked for this, give us guidance, give us tools, and help us. But also help the larger operators and others do even better by, for example, sharing intelligence and better bilateral information sharing. So, that's one of my takeaways is this rebalancing I think is a little problematic.

Tyler Bridegan

Tell me then why, with this rebalancing, are they pivoting to regulations? I mean, what do you think is sort of motivating the White House to take this position?

Lyn Brown

Well, I think the Colonial Pipeline cyber-attack was a wakeup call to policymakers about the potential risk to critical infrastructure. But should Colonial Pipeline be considered the baseline for all industries? Yes, there were gas lines and there were shortages along the East Coast and that's serious. But not all industries are similarly situated. We know, for instance, that rail and the aviation industries have a long history of prioritizing security, preparation, and planning. And I know ONCD is talking about light targeted regulation that is harmonized and highly collaborative and that companies should be regulated once. But is that realistic? Are they really going to tell the SEC, for instance, to stand down and not require public disclosure of material cyber incidents because it's duplicative?

Megan Brown

Yeah, I agree. ONCD, CISA, and ONB I really think need to work hard - and I think they want to - to get agencies on the same page. And this is why, in part, we filed a brief for the U.S. Chamber of Commerce recently in a pretty important case, in which the Securities Exchange Commission is demanding by subpoena that a law firm hand over a client list and files after the law firm was breached by what I think has been suggested as a Chinese nation state based hacking group. And the Chamber's brief there argues that that SEC effort and its theories and assertion of authority here is harmful to federal cyber policy because it's at odds with the many other agencies who are doing, you know, efforts to protect victims, help victims, not punish them or name and shame. So, I had wanted to see more in the strategy about harmonization. There's a paragraph or so. But this is, I think one of the biggest policy challenge challenges for congress and the administration at this point.

Kat Scott

Yeah, you know that said I do want to jump in and talk about some of the things that I think are good in this strategy. I think there are some things to appreciate. So, in several places it recognizes the need for federal agencies to do more on their end to improve basic security. And that's really important here. It also talks about regulation in a way that is helpful. So, when it does talk about regulation, it says that mandates should be based on standards and best practices and those are things - and guiding principles - that we definitely like to see. And then also it calls for investment in U.S. technology and leadership in several areas. So, overall, a lot of concerning aspects of this strategy but some redeeming qualities too.

Tyler Bridegan

So, let's walk listeners through a few highlights of the new White House strategies. So, Pillar One offers ambitious goals to defend critical infrastructure. What are some of the key takeaways that a casual reader might miss?

Megan Brown

Okay, so this is where sort of we dive into the strategy and if people can be patient with the words that the government uses in these strategies, the pillars and the goals and the objectives. But Pillar One has this goal of operationalizing this notion of collaborative defense. That "equitably distributes risk and responsibility." And

that's where this strategy kind of pivots quickly and early to the need for regulation, right? As Lynn had suggested, or said, it suggests the market has poor incentives to invest in cyber and therefore they want to aggressively use existing authorities to close what they see as gaps. But also, they recognize that there are places where they need more authority, where the agencies might not have authority now, so they're going to have to go to Congress. Personally, I question that premise. I think a lot of companies are investing heavily in cyber. I don't think they have an incentive to have their networks go down, data stolen, or operations interrupted. So, it's really kind of - I don't know that it's fair to say that there's inadequate incentives. There's just maybe, you know, more that can be done, and the government can help. And so, anyway, what this means is you're going to see more regulations by departments and agencies. One thing to note: they had a couple sentences in here - I found it remarkable that the strategy would explicitly call for state regulation when the administration has already received some pushback from, ah, for a letter that the president wrote to state governors a while back, calling on them to regulate cyber. And that's precisely the kind of fragmentation that we don't want to see. I would hate to see the state patchwork of data privacy laws flower in the cyberspace.

Kat

Yeah. This pillar also talks about the security of federal systems. And the strategy notes ongoing efforts to implement a Zero Trust Architecture Strategy and modernize IT and OT infrastructure across the federal government. Federal IT security, as we sort of mentioned earlier, has been a perennial challenge. And in light of recent public recognition of federal security challenges and breaches, you know, the federal government may not exactly be the model that the White House envisions for critical infrastructure across the United States for how to successfully build and operate secure and resilient systems.

Tyler Bridegan

Awesome. And then Pillar Two calls for initiatives to disrupt threat actors, which I think every company has been trying to do on their own to some extent. How will that impact the private sector?

Megan Brown

So, the administration says it wants to use all instruments of national power and that's not new, I mean that's been part of every cyber strategy in the past. They want to build on those disruptive efforts by doing greater collaboration and they have some creative ideas in there. But it's really trying to put on steroids some of the collaboration that's already happened.

Lyn Brown

Right. And Pillar Two also says that the Department of Justice will lead federal efforts to integrate federal disruption activities and increase intelligence sharing and victim notification through the FBI and through NCIJTF. The National Cyber Investigative Joint Task Force. But those efforts were also already ongoing and doing quite well, I think. The strategy acknowledges that ransomware is a threat and that it has had a tremendous impact, because it's disrupted hospitals and schools and pipeline operations, as we just talked about, government services, and other aspects of critical infrastructure or essential services. I am glad,

however, to see that they're countering ransom attacks, particularly those from Russia, Iran, and North Korea on key critical infrastructure services and that those efforts will continue to be a top priority.

Megan Brown

There's also a lot of concern in this pillar about misuse or the use of U.S. infrastructure by malicious actors. So, there was already an executive order put out, it's 13984, that this strategy sort of doubles down on. So, I think we can expect to see movement on this executive order, which is really about imposing, know your customer obligations on internet service providers. And I think that's kind of concerning and I think that we'll have to see how they want to tackle that. But I think that's going to be a nettlesome area for them.

Tyler Bridegan

Yeah, definitely. And then in Pillar Three, it looks like the Biden administration announced an intent to what they're calling reshape market forces to drive security and resilience. Kat, could you tell our listeners more about that?

Kat Scott

Yeah, overall, the Biden administration in this pillar really believes that government needs to do more to incentivize industry to prioritize cyber risk management. So, they want to work with Congress to pass national privacy legislation that imposes limits on the ability to collect, use, transfer, and store personal data. The administration plans to work with Congress also on legislation establishing liability for software products and services onto developers and manufacturers. The administration supports a liability safe harbor for software manufacturers. The administration in this effort will offer grants or incentives to help companies build security and resiliency by design. And, similarly, the government will seek to leverage the federal procurement process in this effort to improve accountability. Finally, under this pillar, the administration plans to study whether federal cybersecurity insurance is necessary as a backstop for catastrophic cyber security incidents and looking into whether that should be required. The government already began an inquiry on that last year. But this strategy gives that effort new energy.

Megan Brown

So, I think national privacy legislation and the enhanced software safety liability concepts may prove to be heavy lifts. I'm optimistic that maybe we'll get privacy legislation done but, we'll see. I'm particularly troubled, frankly, by the focus on liability in several places in the strategy and that builds on some ideas from the cyberspace solarium commission a couple years ago. I just think it's the wrong tone to set and encourages organizations in an incident or when a supplier has an incident like in a Log4J or Solar Winds, to think first about blame and responsibility instead of collaboration and cooperation to address the situation. And I just think that's not a great dynamic. I also just don't see the utility of publicly shaming companies or encouraging companies in the supply chain to prematurely take this kind of adversarial posture and immediately be worried about liability and risk and contract terms. It's important, it's there, but I don't know that it should be the first thing that people think of and this emphasis, I fear, encourages that.

Tyler Bridegan

Yeah, that makes sense. So, Pillar Four calls for steps to invest in a resilient future. What should listeners care about there?

Megan Brown

So, Pillar Four talks about this resilient future and taking steps to secure internet protocols. I think they may be a little too pessimistic about the current state of internet security and they don't have a real specific answer there or guide for the agencies about what needs to be done about it. But I was really pleased to see some of the federal research and development activities that they're thinking about to, you know, use DHS and NIST and some of these FFRDCs to promote technology and innovation. And I think that's promising and would support longstanding federal policy about using global standards and letting the private sector come up with the best practices and then roll those out. That, to me, was a nice part of the strategy.

Kat Scott

Agree. And multiple work streams are already underway across the government in the private sector on internet security. So, some of these efforts raise really hard policy and practical and legal questions and may need sustained collaboration domestically and globally. ONCD and the White House may find it challenging to coordinate across these disparate efforts and avoid duplication of that ongoing work.

Tyler Bridegan

Yeah, we've definitely been monitoring all those different works streams. So, Pillar Five talks about international partnerships. So, what does the White House have in mind here and how much of it is really new?

Lyn Brown

So, Pillar 5 moves to the international scene as it outlines important roles for several departments and agencies. So, the Department of State will focus on capacity building priorities with key U.S. partners. DOJ, of course, will focus on global crime. Interestingly, the U.S. will be leading a NATO effort to build a virtual cyber incident support capability to enable allies to respond collectively to cyber threats. As for what's really new, the U.S. has already exercised considerable leadership in fighting international crime. Recently, FBI and DOJ announced the successful takedown of the hive network in coordination with law enforcement entities around the world. This disruption effort reportedly thwarted over a 130 million dollars in ransom demand. So, I think it's fair to say that the U.S. has already been successfully coordinating international efforts to investigate and prosecute cybercrime worldwide. As indicated by the sequencing of these types of disruption operations by FBI and DOJ for the last several years. Utilizing, you know, an all-tools approach to target malicious cyber activities.

Tyler Bridegan

So, a lot going on in the White House strategy. I want to briefly talk about another notable site cyber development at the Department of Commerce's National Institute of Standards and Technology, or NIST. Their cyber security framework. So, that framework is a tool designed to help organizations create cybersecurity programs that align with the organization's risk tolerance at a high level. So, Kat can you give our listeners a preview of some changes to the framework that they should be expecting.

Kat Scott

Absolutely. So that's exactly right. NIST is currently updating the cybersecurity framework or the CSF. Its current version is 1.1 and they're doing an update to version 2.0. They've released a concept paper that outlines what they expect to change in this update and comments are actually due on that concept paper in a few days here, on March 17th. The agency has held several workshops and other activities for organizations to participate and collaborate in this effort and we expect some pretty important changes. Right now, there's a pretty spirited debate going on about some structural changes that would move governance and cybersecurity supply chain risk management up in prominence in the framework. Some sectors and participants don't think that it's a good idea to do that because it may impact backward compatibility of the CSF and that's really important, especially given that dozens of mappings and even foreign government efforts have been built off of the existing CSF and the existing core. So, you know, a lot of folks are cautioning this not to make major changes, to not disrupt those efforts that are built on top of the CSF.

Tyler Bridegan

So that seems like it's an ongoing process that companies should be aware of.

Megan Brown

Yeah, I think it's really important to watch because companies across the economy are going to be expected to use it. The CSF has been very successful. NIST is considering, however, those major changes that Kat said, and I think there's a few real interesting sort of debates going on with the private sector users and NIST. But I think all private sector companies should watch for what pops out over the next year.

Tyler Bridegan

Yeah, that's great to know. It sounds like we'll cover that in a later episode as it develops more. So, in closing and as a teaser for future discussions, what are each of you watching in the next few months on cyber?

Lyn Brown

I'm watching the regulatory rollout and deconfliction efforts just yesterday TSA released new cyber rules for airports and airline operators the new aviation rules track with what we saw with the rail security directives in several ways. Both rail and aviation need a designated cyber security coordinator, a vulnerability assessment, a cyber incident response plan, and a cyber implementation plan focused on "defense in depth that's

approved by TSA." So, I'm following how these new rules will be harmonized or deconflicted with, for instance, the rules that are going to be issued soon by CISA or the SEC.

Kat Scott

Yeah, one agency I'm watching really closely for cyber regulatory developments is the FTC. In addition to the security and privacy rulemaking that I talked about a little earlier, the FTC has been really active with respect to cyber security enforcements lately and they've indicated that they are ready to take a fairly bold and novel position on breach notification obligations. Same goes for cybersecurity expert expectations for general private sector companies. So, I think the pro-regulatory tone of the national cyber strategy is likely to further embolden folks over at the FTC. So, it's definitely an agency to keep an eye on. And I know you only ask for one, Tyler but there's another thing I'm watching really closely and that's at the state level. You know you mentioned this earlier, Tyler that there are new Omnibus privacy laws that have affirmative Cyber Security Obligations baked in. As these laws come into effect this year, it's going to be really important to keep an eye on enforcement trends there.

Megan Brown

Yeah, and I'll sort of grab a 2-for as well. First, in the next few months I really want to see what the federal court in DC decides in the SEC's subpoena fight with Covington, the law firm, and whether the government is going to, you know, in response to that or just more generally try and rein in agencies who are, who are poised to fragment cyber policy. In that case, I think by revictimizing victims of cyber-attacks. And then another piece I want to watch is sort of DOJ's overall tenor. They rolled out this civil false claim's initiative for cybersecurity. And I found that a little troubling at the time because it seems to take a skeptical look at companies and maybe presume some inclination to bad faith. But I think you know there's been very few actions taken under it. But I think that will be really important as well to look at. The government talks about "accountability" kind of what that means, as Kat said, at the FTC and at other agencies. So, lots that I'm looking forward to.

Tyler Bridegan

So, this space isn't active at all is what you guys are telling me.

Megan Brown

Very sleepy, very boring. Nothing to do.

Tyler Bridegan

Not an area of concern for the government whatsoever. So, it really is pretty remarkable how many initiatives are coming out of DC this year. But on that note, I want to thank our guests Megan Brown, Lyn Brown, and Kat Scott for taking time out of their day to join me. And I also want to thank our listeners for tuning in and, as always, please feel free to reach out to anyone on this podcast should you need any further information on the multitude of cybersecurity regulations in the works these days. Thanks everybody.