#220 - EO Updates to AI

G Mark Hardy: [00:00:00] Hey, AI policy in the U. S. has taken an about face through a range of executive orders. Some of them are aimed to strengthen national security and others to remove barriers to innovation. But what does that mean for you as a cybersecurity executive? Which directives still stand? Which have been scrapped?

If you understand these shifts, it's not just bureaucratic housekeeping, it's essential for protecting your organization. Stay with us as we unpack the impacts of these policy on AI, security, and your strategic decisions.

.... hey, since we're talking about AI today, here's an awesome tool that will help your developers leverage artificial intelligence to detect security vulnerabilities in your software. ZeroPath is a SAST tool that can find and fix broken authentication, logic bugs, outdated dependencies, and more. Become secure by default [00:01:00] in minutes with an AI tool that even creates patches for your code rather than just flags vulnerabilities.

Why push vulnerable code when a solution is now a reality? Schedule a personalized demo today at zeropath. com hello, and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G. Mark Hardy. I'm your host for today, and we're going to look at a number of U. S. presidential executive orders, or EOs for short, that relate to artificial intelligence and may impact on your duties as a CISO or cybersecurity professional. Now, first of all, what is an executive order? Now, the American Bar Association offers this definition.

An executive order is a signed, written, and published directive from the President of the United States that manages operations of the federal government. Now, every president has issued at least one, and they're numbered sequentially from the days of George Washington to our current president. And they often [00:02:00] will task different entities of the executive branch with deadlines of 90, 180, 270 days to produce some sort of follow up.

Recommendations, action plans, or even issue guidance. Now, as ABA points out, Executive orders are not legislation, they require no approval from Congress and Congress cannot simply overturn them. Congress may pass a legislation that may make it difficult or even impossible to carry out the order, such as removing funding, but only a sitting U. S. President may overturn an

existing executive order by Issuing another executive order to that effect. Now, these come out in the Federal Register, and they do have the force of law. So let's take a look at some of these EOs that pertain to AI. The first one that I could find that related to artificial intelligence was issued by President Trump in February of 2019.

It was called EO 13859, Maintaining American Leadership in Artificial Intelligence. Now, the [00:03:00] purpose was to launch the American AI Initiative, which establishes AI as a top research and development priority. And it put out a number of key directives, such as promoting AI research and development, basically encouraging federal agencies to prioritize AI investments to drive innovation, enhance access through AI resources by improving data and computing resources for AI researchers, and to set AI governance standards, pushing for an AI friendly regulatory framework to ensure that ethical and safe deployment of AI technologies works, and went out to federal agencies and said, hey, maybe you should start improving your AI workforce skills.

But what's that impact on us as a CISO? It really sets a foundation for AI adoption in government and by extension private sectors because a lot of companies work with the government. It increases the AI integration because it's encouraging organizations to adopt artificial intelligence, which means you have to update your security protocols.

It focuses on data management [00:04:00] by emphasizing data sharing requirements to provide some robust data governance policies. And even some ethics. CISOs shall ensure that AI applications align with ethical standards and don't compromise security. Now, it didn't create any specific cybersecurity mandates per se, but it did help to accelerate AI use across industries, which could potentially increase attack surfaces if you don't have the security in there.

Now, to me, 2019 seemed rather early for a national directive on AI, and in retrospect, it looked like that administration had a unique foresight to anticipate what has now become a highly competitive international subject. But, before we congratulate ourselves, let's look around a little bit. That executive order did not identify specifically any national adversaries, such as, People's Republic of China, or PRC.

Nonetheless, the 13th Five Year Plan for Economic and Social Development of the People's Republic of China, which covered 2016 to 2020, referenced a 2013 [00:05:00] document called Made in China 2025. here we are. And that

included plans to upgrade 10 sectors of the economy, including new advanced information technology and automated machining tools and robotics.

That was the result in part of a 2006 document that laid out a 15 year science and technology plan that addressed an overall strategy for medium to long term science and technology development. So it's no surprise, therefore, that China has made significant advances in AI. Think DeepSeek, as they are in their 20th year of national focus on AI and its precursors.

If you want to look into those documents, as well as any of these EOs, check the show notes. I've got them all on my footnotes. So let's take a look then at EO 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, issued by President Trump in December of 2020. Now, this order focused on fostering the use of AIs in federal agencies.

Emphasizing [00:06:00] trustworthiness and accountability. Some of the key objectives of this executive order were guidance for AI adoption, essentially providing a roadmap for agencies to implement AI responsibly and establishing some principles for AI trustworthiness, fairness, and accountability. Required agencies to assess risks before deploying AI and with respect to public trust, ensure AI use in government maintains public confidence through transparency and accountability.

Well, what are the implications for us as a CISO or a security professional? It introduced early risk management expectations for AI systems. It directed continuous evaluation of AI systems to identify potential vulnerabilities. Sound familiar? Push for explainability and governance, which some organizations adopted as best practices.

It provided some standardized AI practices that could streamline security measures. It focused on transparency as well to maintain clear documentation and communication about AI use to build [00:07:00] trust. And however, it did not mandate cybersecurity protections for AI models, which left a bit of a policy gap.

Now, fast forward. To May of 2021, there's been a change of administration and now Executive Order 14028 is issued by President Biden on the 12th of May, 2021. And this was his first cybersecurity EO, less than four months into the new administration. And it aims to strengthen U. S. cybersecurity defenses for federal networks and critical infrastructures in response to increasing threats.

Now this covered a whole lot more. This is a subject of a lot of discussion that we had four years ago. I did a whole episode on this one four years ago. If you want to go back and look through CISO Tradecraft, you can find it. But some of the key directives were it required federal agencies to adopt zero trust security and enhance software supply chain security by implementing rigorous standards for software development.

Think the. SBOM, Software Bill of [00:08:00] Materials. Established multi factor authentication, or MFA, in endpoint detection standards. Surprisingly, a lot of organizations weren't using MFA properly, and some still aren't. I created the Cybersecurity Safety Review Board, which is modeled after the NTSB with regard to transportation issues and accidents, and talked about improving detection of cybersecurity vulnerabilities by deploying systems to identify and mitigate threats promptly.

If we take a look at ai, a lot of these will apply as well. They're IT systems and it brings up some implications for us. One of them is supply chain vigilance. Ensure your third party software complies with your security standards. Look at the terms and conditions. Did you look at deep seek, for example, great results.

However, the terms and conditions plainly state that your information is going back to and will remain in the People's Republic of China. Now, if that's perfectly aligned with your security standards and your risk. Profile, go for it. But if it's not, you should probably pay attention to things like [00:09:00] that as part of your supply chain.

Incident response planning. It talked about for CISOs and security professionals, we need to develop robust plans to respond to cyber incidents effectively. We want to look at continuous monitoring, implement advanced threat detection, safeguard your assets. It also offers some clear cybersecurity best practices that a lot of private companies went ahead and followed because they said, Hey, this is not a bad idea.

Push software vendors to improve security transparency. Again, a lot of that through the SBOM. And also strengthen cloud security expectations, which I think is a little bit more relevant, because as AI adoption has increased, most of these models are run in the cloud. Fast forward to 2023, Executive Order 14110, the safe, secure, and trustworthy development and use of artificial intelligence.

And this was published in October of that year by President Biden and creates a national framework for AI security, ethics, privacy, and really focuses on ensuring AI [00:10:00] technologies are developed and used in a manner that

protects public safety and national security. Now, what are some of the key directives here?

Required AI safety testing and audits for high risk applications. Enforced privacy protections in AI systems handling personal data. Established AI governance standards for federal agencies. Encouraged research into AI cybersecurity threats. And promoted some innovation. Encouraged the development of AI technologies that will benefit society.

from that EO, what can we think of as a CISO? now you have security and transparency expectations. That are placed upon you and a lot of organizations said, good idea. We'll get ahead of any laws or requirements and we'll just go ahead and adopt that. Also laid out a national risk assessment method for AI based cyber threats, created compliance requirements for adhering to a new safety and privacy standards and AI deployments, looked at data protection, enhancing measures that protect sensitive information used in AI systems.

And a little bit of [00:11:00] balancing security and innovation by fostering a culture that encourages innovation while maintaining robust security protocols. Now, that sounds pretty good. However, EO 14110 was revoked by President Trump by Executive Order 14148. Initial rescissions of harmful executive orders and actions signed on January 20th, 2025. Now we do not get into politics here at CISO Tradecraft, but I did find it interesting that this EO was swept up with a number of other Biden administration EOs that would more likely be identified by the differences in governance between the two administrations, such as EO 13985, Advancing Racial Equality and Support for Underserved Communities Throughout the Federal Government, or Executive Order on Preventing and Combating Discrimination on the Basis of Gender Identity or Sexual Orientation, or even Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis.

Now, lest you think that creating a policy seat change on Inauguration Day is a brand new concept, note that all three of these executive orders were enacted on January 20th, [00:12:00] 2021. So this new EO seems to leave a gap in U. S. policy toward A. I. security as it has rescinded a lot of that, but a mere three days later, President Trump signed EO 14179, removing barriers to American leadership in artificial intelligence.

Now, this purpose as stated is, quote, this order revokes certain existing AI policies and directives that act as barriers to American AI innovation, clearing a path for the United States to act decisively to retain global leadership and

artificial intelligence. that sounds pretty good. And it goes on to include a one sentence policy statement.

It is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security. Now, how are you going to get there from here? Some of the key objectives were [00:13:00] deregulation. It removed policies that were considered by the new administration to be obstacles to AI advancement.

promoted innovation by encouraging rapid development and deployment of AI technologies, and was designed to enhance competitiveness globally by positioning the U. S. as a leader in that AI landscape. But it also ended federal AI safety assessments, it eliminated mandatory AI risk management guidance, and it shifted the AI strategy from secure AI to unleash innovation.

Now, By revoking EO 14110, that signals that the government mandated AI safety regulations are not moving forward as initially planned and therefore organizations probably need to set their own AI security standards instead of relying on federal guidance. Although you can still refer to the prior EO, there's nothing that says you can't do those things unless you're in, of course, the federal government.

And then [00:14:00] ethical AI and cybersecurity concerns are now potentially a corporate responsibility rather than a national directive, meaning that it's up to us to recommend to our executive team how are we going to address ethics and cybersecurity with respect to AI. So as an impact on our CISOs, we don't have this federal AI security mandate.

You've got to define your own framework. Although as I said, utilizing what's out there in the federal government's already pretty good idea because if you say, Hey, I use a NIST framework, Much fewer people are going to. Complain, then if you say, I'm using my own personal framework. AI adoption is going to accelerate.

It's going to continue to do but the security risks may increase with the lack of these protections that are in there. And organizations are potentially going to have to self regulate AI vulnerabilities rather than following federal standards. This EO is not designed to release chaos, rather it tasks the assistant to the president for national security affairs, the special advisor for AI and crypto, [00:15:00] the assistant to the president for national security affairs, to coordinate with the heads of executive departments to realign provisions of the

EO 14110, remember that's one that got revoked, with this new policy statement within 180 days.

So I'm going to expect further federal guidance coming out on this subject. Now, before we wrap up on that and say, that's everything we want to think about. Yeah, you thought you'd get off early on this episode. There's a squeaker, EO14144. Now that is interesting because it seems that the new administration came to work on day one loaded for bear.

However, on the 16th of January, just four days before inauguration, President Biden issued this executive order strengthening and promoting innovation in the nation's cybersecurity, which builds on executive order 14028, which came out in May of 2021. Remember, I did an episode on that, improving the nation's cybersecurity, and that was not affected.

By the [00:16:00] change of administration. So this departing EO states as part of its policy, quote, I am ordering additional actions to improve our nation's cybersecurity, focusing on defending our digital infrastructure, securing the services and capabilities most vital to the digital domain, and building our capability to address key threats, including those from the People's Republic of China.

there we go. They're calling up PRC directly. Back in the old Wild West, thems be fighting words. But at the time, at the end of administration, it could neatly sidestep any potential disagreement between China and the incoming administration, allowing the United States a little bit more of a free hand to pursue their strategy.

So in a way, played. Now this EO is probably the longest one of all the ones that I have looked at. And if we take a look at what's in there, we're going to find out that there's a lot that comes into play with regard to this executive order. It talks about fortifying software supply chains.

We have [00:17:00] insecure software. It's a major problem. We talked about SBOMs previously, and the fix is that software providers have to submit machine readable attestations and high level artifacts to CISA, which are going to prove their adherence to secure development practices. Okay, that's that's a big deal.

So as a CISO, you need to demand that your software providers participate in the CISA repository for software attestation and artifacts program called the RSAA. Do some rigorous risk management. Don't just trust, verify. And then do

the continuous monitoring. We mentioned that a couple of times. They're your software providers are not only attesting to the secure practices, but they're actively fixing known vulnerabilities.

What else is in there? Elevating secure software development practices, because just having software isn't enough, and having somebody go back and patch bugs isn't enough. It really needs to be secure by design. Now, the National Institute of Standards and Technology is leading a consortium to develop guidance based on the [00:18:00] NIST Special Publication 800-218.

Secure Software Development Framework, or SSDF. So as a ciso, what do you wanna do? You wanna get your developers to start implementing the SSDF in your software practices. Stay up to date with NIST Special Pub 800-53, rev five at least for now, and make sure that you have all of those things that you have identified as controls installed.

And keep your patching up to date and continuously get better at that. How about for cybersecurity supply chain risk management? adversaries are targeting weak links in supply chains for federal agencies and quite honestly also in corporate agencies as well. Smaller companies, smaller suppliers don't have the resources of a Fortune 500 company or a federal agency to protect.

Therefore, why not go after the weakest link? And so agencies, the federal government have to integrate cybersecurity supply chain risk management. Adhering to NIST Special Pub 800-161. Now, again, if you're not in the federal [00:19:00] government, you're going to say, it doesn't apply to me. You might want to think about this because these are good ideas.

So from a risk integration perspective, integrate cybersecurity into every stage of your acquisition lifecycle, from planning to performance evaluation and annual updates to OMB if you're a federal agency and you're progress in implementing your SP 800-161. How about open source software? Open source software it's great. However, there's a, almost a religious argument between open source and closed source. Open source, the one side, it says, everybody can take a look at it. If there's any bugs or problems, it'll become known and we can patch it. The flip side of that is, bad guys might be able to find a lot easier problems and exploit them until such time as they're patched.

On the closed source, we have something like a Microsoft. I guess it's better because nobody can see the code. They don't know how it works. But the flip side of it is, that all these really smart security researchers out there may not

have access to [00:20:00] the tools to be able to add to the body of knowledge of people trying to fix stuff.

So again, that's a religion problem. I don't try to solve that one, but just be aware that there's two sides of the issue. But what's coming out of that is CISA and OMB are going to issue recommendations on the security of open source software. So if you're using open source. Have a robust process for security assessments and patching.

And, think about OpenSSL. that was open source. It was just a project that a couple of people did, and it created massive vulnerabilities. Why? Because people had found out that, it gets embedded in a module, which can embed another piece of code, and piece of another piece of code, and it might be three or four layers back before you find that.

I love what Google did about that. Everybody's complaining about it. How can we have such a horrible vulnerability? And someone realized, just Two guys working on it in their spare time, instead of complaining about it, Google said, Hey, if we give you 50, 000, I think that was the amount. Would you like not worry about your day jobs for a while and just go fix this thing and solve it for the world?

[00:21:00] Pretty cool. So contribute to open source projects, help out with their security, do things like Google did, that's going to be a great thing. Federal systems, because, federal systems really need to adopt best security practices. They don't always have access to the right resources, but agencies need to prioritize innovative identity technologies like phishing resistant authentication, strengthen your cloud security.

here's my phishing resistant authentication right here. For those who are watching on YouTube, my. YubiKey, and I have found that works quite well. Not that I'm too worried about getting phished myself, but I'd like to leave my example. So that's what I do with my systems. And also, for recommendations, pilot deployment.

How about, WebAuthn or something like that as a phishing resistance standard? hardware tokens like YubiKeys, all these things you can do to go ahead and reduce Likelihood that your people are going to be phished for credentials. Improve on your threat hunting capabilities. Go out and look for identify threats using CISAs capabilities and put [00:22:00] specific protections in place for highly sensitive data because we know that's pretty much what the bad guys are coming after.

How about securing the cloud? Because cloud security is really important for a lot of organizations and particularly in the federal government. I remember the move to the cloud came out in the Obama administration and that was a push to go ahead and start using cloud resources. here we are over a decade later, and now it's a way we do business now.

FedRAMP, Federal Risk Management Program, it's going to require cloud service providers to produce baselines with configurations Agency cloud based systems. Okay, that sounds like a good thing to do. So if you are using cloud services and you are in the federal government, you need to make sure they meet FedRAMP requirements.

You have secure configurations. And oh, by the way, even if you're not in the federal government, what's good for them might be good for you. And you might want to emulate some of those controls. And then another interesting thing, they talk about space systems, which are increasingly under threat because new civil space [00:23:00] systems need to use a risk based tiered approach for cyber security.

I remember when some of the early satellites went up, I worked on a project. Back in the 1980s, I guess it was around 1988, 87, I worked at the office of naval research and there was a program out there called Spinspat, special purpose, inexpensive Navy satellite, or single purpose, inexpensive Navy satellite.

I've been about almost 40 years, so I'm not sure I remember the exact name, but basically the way it worked was, is that, there's one little division in the Navy said, we're going to put stuff on orbit. And it's going to weigh less than one or two kilograms. It's these little, how do we get them up on orbit?

We don't have rocket launchers. So basically they had some Navy captain going around trying to hitch a ride and said, how much room you have left for your payloads on this Ariane rocket? they can hold. Maybe an extra 1, 827 grams that we'll book it and then we'll go ahead and build some little project or have something you can get up on orbit and do that.

What was interesting is that my job being the cyber security guy [00:24:00] was how do we protect the telemetry information? How do we protect these experiments? Because somebody else might a listen in on it or B try to take over the command and control. So I got together with the folks over at the three letter agency called NSA.

And said, Hey, here's a business requirements. I'm being presented with. We need to put these little satellites up on orbit and they need to be protected with regard to security and stuff like that. We said, no problem. We have just a solution for you. So I've got this little tiny satellite that I'm going to go ahead and put up on orbit.

I figured, okay, fine. This is great. And they come back with this big steel plated, armor resistant, gigantic device that weighs about 10 times as much as the satellite itself saying, this is the. KY 123 that will protect it. It's no, it's, we can't get that thing on orbit. Can we just get the code and the software and the chip or whatever?

Nope, nope. Can't do that. So we ended up just launching them and figured that, okay, we're going to experiment. If somebody screws with it, they screw with it. To my knowledge, nobody [00:25:00] did. But today there's a lot more capabilities out there for people to mess with stuff. And so we want to think about safe space.

there's my C story for the episode. So what we want to do is have a risk based approach to space system security. If you're in that space, think about on orbit link segments and robust control of command and control encrypted, authenticated. The nice thing is we can do all that in software. You don't need a big guy, NSA armored device to do that.

It also gets into some nitty gritty and government communications, like internet routing security, talking about BGP, Border Gateway Protocol. And I remember doing an episode on Border Gateway Protocol several years back. Why? Because I really wanted to learn about it. By the way, the best way to learn about something is to teach it to somebody else, because you have to research the daylights out of it.

So if somebody asks you questions, you can answer them. And The fix here is that agencies have to use registration service agreements, publish route origin authorizations, and use Internet routing security technologies. what does that mean to you as a CISO? Look at the regional [00:26:00] registry. Make sure all your IP address blocks are covered by a registration services agreement.

Create and publish route origin authorizations for all of your IP address blocks, and then look at your contracts. Make sure there's language in your contracts that require providers to adopt Internet routing security technologies. Also encrypted DNS, because unencrypted DNS traffic is a major vulnerability.

Typically we use port 53, UDP, although it can be TCP. I think if you're going to be over 1024 bytes in the response. So there's your little Hacker Jeopardy question for the day. And so the thought was, is that all DNS resolvers must support encrypted DNS. Now we're not talking DNSSEC, we're talking about encrypted DNS, which means if you implement those protocols wherever you can, and make sure that you have it with any contract, With a Contractor that has DNS resolver, you'll be farther ahead.

for example, Cisco Umbrella will do DNS encrypted. They don't do port 53, they do port 443. I'm not [00:27:00] going to dive into the technology. But the whole idea is if somebody's listening in on your DNS, they can't intercept it, come up with a fake answer, because they're not going to break the crypto. Other things.

Email encryption. This thing about email is a major point of compromise, so agencies have to enforce encrypted transport between email clients and servers. If you're using Microsoft Exchange, it's probably done by default, unless somebody has turned that off, and I hope not. make sure you encrypt and authenticate at the transport layer, all your email connections, and If you have your own email servers, make sure that's turned on there and server to server as well.

If you're up in the cloud using a major provider, a lot of that is turned on by default. But check the defaults just in case somebody has accidentally or deliberately thrown a switch. How about modern communications encryption? Voice and video conference are often lacking end to end encryption. And so this is one of the things we found out.

Salt Typhoon was demonstrating that adversaries were in the United States national [00:28:00] infrastructure, able to go ahead and get content. If it wasn't encrypted, it's theirs. Now, if it is encrypted, we're talking about the concerns about quantum, which we'll get into probably. And some other episode, and we've talked about it before, but essentially, if you say, hey, I'm in quantum, I actually got that coming up, I'll talk about quantum, next, so for end to end encryption, make sure it's encrypted for voice, video and messaging, you log all that stuff, even if using end to end encryption, but as they say for quantum, What's a concern?

We're talking about post quantum cryptography or PQC. Now, what type of crypto is vulnerable to the quantum computing? It's not the symmetric cryptography, like using AES or something like that, or DES, even for those

who remember that, or triple DES. Why? Because those are cyclical ciphers that go through multiple iterations.

Rather, what's vulnerable Is your asymmetric key cryptography, which relies usually on a mathematical [00:29:00] problem, which, if you could create a quantum environment where all solutions exist simultaneously, like factor this gigantic integer into two prime numbers, RSA. All of a sudden, you can do that with quantum.

I can't do it today, so what's my vulnerability? Because an adversary can record all those communications, and in a year, two, or however many years before it's viable, go ahead, run those key exchange through their quantum computer, figure out what the private key was, and then decrypt the correspondence.

Now, for the most of us, 99. 99 percent of what we talk about is going to be totally irrelevant in three to five years. However, that 0. 01 percent might be incredibly valuable if it has to do with strategic assets or special weapons or something like that. And so getting ahead of that problem now, if your board says, we're not going to fund you because it's not a current threat, point out about the fact that you're [00:30:00] inoculating yourself against a threat that's coming down the line.

So when possible, use post quantum cryptography. Make sure you're at least up to TLS 1. 3, meaning that 1. 2, which is still valid. Stop using it. Just upgrade everything and then look at commercial technologies to help protect stuff like hardware security modules, HSMs to protect your keys. And there's even more stuff with regard to cybercrime, like digital identity, talking about synthetic identities, stolen identities to defraud public benefit programs.

We saw a. Fortune go out the door during the COVID benefits that were offered. boiler rooms were set up in certain countries in Western Africa were just like a call center. It compensated, okay, this next thing here's your name and here's your state. And here's your script. Hello. Hi, my name is Bill Smith and I live here in Seattle, Washington, and I lost my job due to COVID and I need a benefit.

And once you finish the call, the next one comes up. Hi, I'm Tommy Jones. I live here in Tupelo, [00:31:00] Mississippi, and I lost my job and I need to apply for, and it's just all day long. And he's pumping the federal government and the state governments for hundreds of millions of dollars. I've had digital identity documents for public benefit programs.

that would be great. Remote verification, interoperability, private seat protection are all ways that we could ensure that we do that. But the interesting thing is that there does seem to be a big political debate about digital identity. And some people are worried about an Orwellian 1984 state.

Other people on a perhaps, less honorable basis are saying, hey, how are we going to vote early and often if you require everybody to produce a unique identity? Again, I don't get into the politics on this. I just point to the issue and then we'll walk past it and go. All right. Also, identity verification methods can be invasive.

The woman says, hey, you go to a bar, for example, and the, the bouncer asks some young lady to say, do you have your ID? Let me use that gender for purposes of illustration. And now the person, okay, here, I've got my ID. And you're like, [00:32:00] ah, so you live at one, two, three main street and your birthday is next week.

And, I don't know. Maybe I'll come by. And she had to cough up all that information just to get in the bar. Would you want as a way to be able to say, prove to me that you are of drinking age? That's it, yes or no, all of the other details are not relevant. And if you're valid in, if you're not valid, don't go in.

And I work on a problem. Wow. About five years ago, with a client who is over in a different country, actually in Australia, that was trying to implement that. And I wrote a whole bunch of protocols for that. I don't know if their product ever went anywhere because I was doing the foundational work, but the whole idea was just to create something using identities and managing that, with regard to keys and public keys, et cetera.

So you could. Just say exactly what the other person needs to know, but no more. The idea of an attribute validation service and preserve privacy. So this has been going on for a few years, but this is now formalized as of January 2025 from the federal government. And then payment [00:33:00] notifications. would you like to know if your identity is used to request a payment?

Because fraudulent transactions will go unnoticed for a while until all of a sudden you find out, Hey, my credit rating is horrible, or someone's repossessing my house or something terrible because you've been the victim of identity fraud. So there's an effort to go ahead and create a pilot program for that.

But stay ahead if you run payment systems, make sure you monitor them and you validate them regularly. A couple other things that were in there, AI for cyber defense, because traditional methods aren't enough against sophisticated actors. So we'll create a pilot program for AI enhanced cyber defense in the energy sector.

And implement these solutions in your strategy for cyber defense and look at the vulnerability detection, automatic patch management, anomaly detection, there's a lot of things that you can do and for additional research into AI and cyber security, prioritizing funding for research into human AI interaction, coding.

assistance for AI security and been secure by design. [00:34:00] And, a couple other things in there. outdated IT infrastructure. It's a huge risk, not just for the federal government, but for any organization. And so on these tasks are modernizing federal information systems, provide some guidance. Some of the things that you can do, migrate to zero trust architectures.

So that you validate everything and you encrypt everything. Use EDR or XDR or question mark DR or whatever the next generation is to keep track of your endpoint and respond to the problems that take place. And look at your vendor management problems. And also think about what do we do with regard to cybersecurity practices?

There should be a minimum, misguidance on minimum practices, comply with them and require your contractors to follow a minimum cybersecurity practice and perhaps go to United States cyber trust mark for consumer internet of things or IOT stuff. And for the most part. we need to protect ourselves.

[00:35:00] We got a call to action here for all of that stuff. And this comes out of that EO that, entitled promoting security with and in artificial intelligence is section six. And again, the title of the whole thing is going to be strengthening and promoting innovation in the nation's cybersecurity. So I covered a whole bunch of areas and I tried to address that to AI, but let me just read you a little bit of what's in section six.

Not all that long. It states the federal government must accelerate the development and deployment of AI, explore ways to improve the cybersecurity of critical infrastructure using AI, and accelerate research at the intersection of AI and cybersecurity. Now this section of the EO directs DARPA. The Secretary of Energy, the Secretary of Defense, the Secretary of Homeland Security to launch a pilot program involving collaboration with private sector critical

infrastructure entities is appropriate and consistent with applicable law on the use of AI to enhance cyber defense and critical infrastructure in the energy sector.

It tasks the [00:36:00] Secretary of Defense to establish a program to use advanced AI models for cyber defense and the National Science Foundation is directed to prioritize funding for their respective programs. that encourage the development of large scale labeled data sets needed to make progress on cyber defense research.

And the Secretary of Commerce is told to prioritize research in four areas. Human AI interaction methods to assist defensive cyber analysis. Number two, securing of AI coding assistants, including security of AI generated code. Methods for designing secure AI systems. And methods for prevention, response, remediation, recovery of cyber incidents involving AI systems.

Awful lot going on here. And the last of this section tasks the Secretary of Defense, Department of Homeland Security, the Director of National Intelligence to incorporate management of AI software vulnerabilities and compromises into their respective agencies, existing processes and interagency coordination mechanisms for vulnerability management, [00:37:00] Including through incident tracking, response, reporting, and sharing indicators of compromise for AI systems.

Now, those tasks are still valid under U. S. law in spite of the change of administration. So we should start seeing results in 150 or 180 or 270 days depending on the agency involved. Okay, so we, let's go ahead and map some of these executive CIS control framework. So we can see what impact they might have on you as a security leader.

Now, With federal AI security mandates rolling back temporarily as ordered by the EO 14148, CISOs are going to have to lead the effort to safeguard your AI systems. So let's take a look at some ideas with regard to the framework of CIS controls. Software and supply chain security, controls 1, 2, 4, and 16. Because the revoked EO that was planned for secure AI software development supply chain protections is no longer there.

So software corporate diligence is going to be a matter of what we do. Integrity is going to depend [00:38:00] on how well you do your stuff. So require your vendors to submit security attestations, align your AI development with the NIST secure software development framework, and require rigorous third party security assessments on your AI vendors.

How about Continuous Vulnerability Management, Control 3? There's no federal mandate now that ensures AI driven systems follow the structured vulnerability patching. automate your AI model updates and security patches, conduct continuous AI vulnerability testing for bias, adversarial manipulation, and exploitability, and use threat intelligence feeds to identify AI related vulnerabilities.

What about identity and access management? Control number five, AI models are often going to process sensitive data, yet the access controls remain inconsistent. So implement zero trust identity frameworks for AI related systems, enforce your phishing resistant multi factor authentication for all your AI model access, and limit your AI admin privileges using traditional [00:39:00] role based access control, or RBAC.

What about data protection and privacy? Control number seven. See, the revoked privacy directive leads to some gaps in the analytics. So encrypt all your AI handled sensitive data sets. Even if you're not told to do do it. Monitor your AI systems for unauthorized data, access or retention, and deploy privacy enhancing AI models, basically federated learning.

Secure cloud and infrastructure controls 8 and 11. Now this federal guidance on AI cloud security has been rolled back. So require FedRAMP certified cloud environments for your AI workloads. Use zero trust architecture for your networks to protect your AI infrastructures. Conduct regular AI system pen testing in cloud environments.

And how about control 14? Secure AI model development monitoring. This is now an enterprise responsibility. It's no longer required. Because from this EO, which is no longer valid. And so as a CISO, establish your secure AI development life cycle. [00:40:00] It's called SAIDL practices. Continually audit your AI model for fairness, security and bias.

Then do adversarial AI testing to be able to detect manipulation threats. So what can we conclude here? The recent EOs illustrate a fundamental shift in AI security policy. The early executive authors Promoted AI adoption, but they lack security mandates. Executive order 14028 strengthened cybersecurity, supply chain security and zero trust, and it's still in force.

Executive order 14110 introduced a lot of AI risk governance, but that was revoked. By the subsequent Executive Order 14179. And with deregulation, AI security depends a lot on private sector leadership. So what are some key

takeaways for you as a CISO, as a security leader? Establish your own internal AI security standards.

The government mandates are not going to help. They're not going to force on it right now. That said, [00:41:00] use these existing government risk frameworks when possible, as well, things that go away by themselves can sometimes come back by themselves. Secure your AI supply chains and software development.

Implement zero trust for your AI model access. Harden your cloud environments for AI workloads. Continuously monitor your AI for vulnerabilities and bias. Enforce robust AI software and supply chain security practices. Integrate zero trust and AI specific access controls. Strengthen your data privacy measures and AI analytics.

Monitor AI vulnerabilities continuously and adapt security postures accordingly. And do secure AI development and deployment. Ensure your models are resilient against adversarial attacks. Bottom line, consider for now that AI security is now a CISO driven initiative. It's not a federal regulated one.

Your organization's AI future and your success depends on proactive security strategies. You're not going to have to [00:42:00] rely on government oversight at this time. Okay, a lot of detail. Hope you found this helpful. The regulatory landscape is shifting and AI security is, it's now in your hands. So stay ahead of the curve.

Implement the CIS controls, prioritize AI resilience, keep your organization secure in an era of deregulation. So I hope you found this helpful. If you like our CISO Tradecraft podcast, make sure you're following us. We're on all the major podcast channels. We're on LinkedIn. We put up more than just a podcast.

We also have a Substack newsletter, which is very popular now. It's really kicked in and let us know, give us some feedback. Say, Hey, we love it. We all like it. I've got some issues with it. You can contact us best way to contact us on LinkedIn. We'll respond back to you and we'll engage in a conversation because we think that this is very important and it pertains to much of us out here.

So until next time, this is your host, G Mark Hardy. Thank you for [00:43:00] being part of CISA Tradecraft. Until next time, stay safe out there.