

July 5, 2026

The President Who Hated State AI Laws Creating an Approval List for Using AI Software

One of the things the president railed against when he first took office was state laws restricting what AI companies can do, particularly with your data. He even signed a memo telling the justice department to sue states that put restrictions on AI companies. Now he has made a 180 degree turn, effectively banning Anthropic's Mythos and Fable by restricting access to it by non-US citizens, even in the United States. He has now said that he will allow a select list of a few companies that he approves of to use Mythos. At the same time China's Zhipu AI has released GLM 5.2 which has functionality close to Mythos. As of last week he had not banned OpenAI's competitor to Mythos and I suggested maybe that is because OpenAI was a donor to the president. Well, apparently, even that doesn't help as OpenAI is "VOLUNTARILY restricting access to its new model" that competes with Mythos to companies approved by the president. **See more details below.**

Please check out our blog at <https://www.cybercecurity.com/cyblog>

You can also find copies of the weekly newsletter at <https://cybercecurity-mitch-tanenbaum-blog.com/SNU>

We have a YouTube Channel with a lot of videos. Check it out at: [Turnkey Cybersecurity and Privacy Solutions, LLC - YouTube](#)

As part of our YouTube channel we have a demonstration of our AI capabilities. The CyberPulse Scoop is an AI driven cybersecurity interview. Click on PODCASTS once you are in our YouTube channel and then on CyberPulse Scoop.

If you received this email from a friend and want to receive it directly, please send an email to Mitch@CyberCecurity.com.

Thanks for your interest. If we can provide any assistance, please let us know.

Video Blogs

We also have a video and audio blog, including an RSS feed at <https://cybercecurity.us>. Not only are there audio and video versions of the weekly security news updates there, with extended commentary, but there are also other blogs about subjects of interest. Please check it out and let us know what you think.

Security/Privacy Alerts

Argo CD Flaw Exposes GitOps as CRITICAL Resource

This is only one example, but it shows how your software development infrastructure could be compromised to allow attackers to compromise your entire production environment. If this concerns you, please contact us. Credit: [CSO](#)

AI Alerts

Check out our Certified AI Governance Leader Course at [AIGIP.AI](#).

The President Who Hated State AI Laws is Now Creating an AI Approval List for Using AI Software

One of the things the president railed against when he first took office was state laws restricting what AI companies can do, particularly with your data. He even signed a memo telling the justice department to sue states that put restrictions on AI companies. Now he has made a 180 degree turn, effectively banning Anthropic's Mythos and Fable by restricting access to it by non-US citizens, even in the United States. He has now said that he will allow a select list of a few companies that he approves of to use Mythos. At the same time China's Zhipu AI has released GLM 5.2 which has functionality close to Mythos. As of last week he had not banned OpenAI's competitor to Mythos and I suggested maybe that is because OpenAI was a donor to the president. Well, apparently, even that doesn't help as OpenAI is "VOLUNTARILY restricting access to its new model" that competes with Mythos to companies approved by the president. They did this "at the REQUEST" of the White House", meaning if they didn't, they would get the same treatment as Anthropic. So what started out as no regulations on AI has turned into a state controlled distribution of AI software. As I said last week, China is thrilled because they are filling that gap as fast as technically possible, distributing software with maybe not quite as sophisticated as US software but definitely sophisticated enough for Chinese state hackers to use against us while most US companies are prohibited from using the best defensive tools available. And, much of China's software is being distributed as free open source software, meaning anyone can download it and some of it can be easily run locally on your computer. China is definitely winning this battle right now. Details at [Metacurity](#) and [Cybersecurity Dive](#)

Table 5 Won't be Available Under Subscriptions After July 7

Don't say I didn't tell you. As AI companies are losing billions of dollars, they are running out of money. While Fable was restored this week, Anthropic says that use of Fable will be "restricted" due to high demand. ***They also said that Fable will move to usage-based billing next week.*** They say it will return to subscriptions some time. Credit: [Bleeping Computer](#) On top of that, Fable has been neutered, according to users, so more expensive and less functional. Credit: [Bleeping Computer](#)

CMMC Q&A

I get to listen to hours and hours of webinars every week, so you don't have to. We are seeing the agencies beginning to get on board and their view of the universe is CMMC Level 2 third party assessment (eventually) for everyone. If you are not already on board this train, the train has already left the station. If you need assistance, please contact us.

We have ITAR data; how does that interact with CMMC?

ITAR is a whole other kettle of fish. ITAR is managed by the State Department. While controls for CMMC and ITAR overlap, they are not the same. You can have ITAR documents that are not covered by CMMC and you can have an ITAR that your CMMC environment does not adequately protect. Can you have a single solution that handles both? Absolutely, but do not assume. Penalties for ITAR failures can include up to 20 years in prison.

We are adding a printer into my CMMC environment AFTER my assessment. Does that trigger the requirement for a re-assessment?

Likely it does so consider what you make in scope or out of scope. Changing things after your assessment is dicey at best. If you have questions about this, contact us. If you are able to do a self assessment then the cost of the re-assessment is probably manageable, but if you have to have a third party assessment, it is going to get expensive after the fact.

DoD Exceeds Expectations For Year 1 Third Party CMMC Assessments by 200%+ Half Way Through Year 1

DoD wrote in the CMMC regulations commentary that they anticipated that 500 companies would achieve their third party CMMC certification in the first year. Half way through that first year we are at more than 1,700 certifications and setting records every month for the rate of new certifications. The DoD is not releasing the number of self certifications, but you should assume that it is some multiple of that. Add the two together and by the end of the year we likely will have 30,000 or more businesses with one of these two certifications. Add to that the fact that we are running our assessors at nowhere close to capacity and we will likely see 6 times DoD's first year planned number of third party certified companies. If you are not one of them, the DoD will likely have sufficient other companies to choose from. If you are still hoping this will go away, all you need to do is look at the numbers and the release of the draft FAR CUI rule to see that the only thing going away will be you if you don't get certified. If you need assistance, you are way behind the power curve. Call us now.

Legislative and Legal Activities

Dutch Crypto Platform Shuts Down; Keeps 30,000 Customers' Money

I can't say this enough. Crypto is dangerous and if you are playing with more than your lunch money, you need to understand the risk. If you are fully informed and still want to risk it, more power to you. I am not sure their customers understood this. The EU has a regulation called MiCA for crypto platforms and they were not able for some reason to obtain the license they needed under MiCA, so their only option was to shut down. Initially, it was orderly but then it collapsed. Dutch prosecutors asked the court to step in and declare the platform bankrupt. Is there any real money left - unknown? If there is, is it say a penny on a dollar? If they have, say \$300 million in liabilities and \$3 million in assets (both made up), then, potentially, a penny on a dollar is the best unsecured creditors will get. Customers are unsecured creditors in the crypto world. Investors will likely get zero. Often the process to get your pennies will take years. Caveat Emptor, as they say. Credit: [Web 3 is Going Great](#)

Education

Are AI Notetaker Apps a Legal Risk for Wiretap Litigation?

The short answer is yes. It depends on whether all participants have given informed consent. This is different from someone noticing that, for example, Firefly is in the meeting. That is not informed consent. This gets really tricky when the app then sends the recording to the cloud for use in training the vendor's AI or further processing. This is a very new area of the law, so watch carefully. Credit: [Galkin Law](#)

Breaches

Note: I could probably report on a hundred a week, but that would make for a very long report. I will, at least, mention a few of the high-profile ones. NOTE THAT THIS IS THE ONLY SECTION THAT I CAN FILL TEN TIMES OVER EACH WEEK.

Hackers Leak Data on 310 Million Temu Users

Temu is a Chinese shopping site that sells pure crap for low prices. If you buy there, and tens of millions of Americans do because they are lured by the prices, what you get is pure garbage. Now you also get your data compromised. Hackers are selling the data and it appears to be recent and legitimate, but Temu has not confirmed the breach yet. Given they are Chinese, they

don't have any requirement to. Data seems to include names, addresses, phones and weakly encrypted passwords. Credit: [Cyber News](#)

Supremes Issue a Ruling FOR Privacy

A 6-3 ruling from the Supremes says that law enforcement needs a warrant before asking the likes of Google or Verizon to conduct a geofenced search. Apparently, a geofence search is too close to the "general warrant" that British soldiers used on the colonists that caused the revolutionary war. Learn more [here](#).

ALERT: New Rules for ALL Federal Government Contractors

If you have been watching from the sidelines as your fellow contractors who have DoD contracts have been struggling with complying with CMMC, get ready. There are new (proposed) rules that will impact ALL federal government contractors. Learn more [here](#).

Google Makes Dev Pay \$11,000 Even Though THEY Told Him he was Hacked

This is a challenge for cloud users and, it seems, that Google is the worst. If you get hacked, you are liable for the bill and there is no way you can put a cap on your charges unlike with Amazon and Microsoft. If you have any cloud services that charge based on usage, you should check what the rules are and whether you can put a cap on your liability. If you need assistance, please contact us. Learn more [here](#).

Security News for the week ending July 3, 2026

This week's news: hackers steal \$75 million from crypto platforms just last month, Apple's hide my email doesn't actually hide your email, Apple is feeling the AI heat too - going to have to make changes, Apple is not alone - be prepared for additional patch Tuesdays and most cybersecurity workers have been told to conceal a breach. Learn more [here](#).

There are new rules coming for all federal government contractors. If you need assistance with this, please contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663