

June 14, 2026

President Gives China Gift Towards AI Leadership

Different people will have different opinions about the president's reasoning for telling Anthropic to shut down Fable 5, its newest AI model, but there is some reality here. If the president wants the US to be the world leader in AI, shutting down the development of and use of our leading AI software is not the way to do that. Perhaps the administration will come to its senses, but in the meantime, Anthropic has turned off its newest AI model. The administration says it is a national security issue, but just like the government's spectacularly failed attempt to kill off encryption in the 1990s, this is also doomed to fail. What the government did was issue an order saying that a license is required for each copy of Fable 5 which is used by someone outside the United States (an export) and also prohibits non US citizens from accessing Fable from inside the United States. This includes Anthropic employees, some of whom are Chinese and many of whom are outside the United States. If those people can't work on Anthropic software they will likely go to work (since they are outside the US) for companies in other countries (like China) that compete with our hoped-for dominance in AI. **Continued below.**

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

You can also find copies of the weekly newsletter at <https://cybersecurity-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://cybersecurity.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.

This week there is a new video on AI - it is here to stay. Lead. follow or get out of the way, because it is coming for you.

Security/Privacy Alerts

President Gives China Gift Towards AI Leadership

Different people will have different opinions about the president's reasoning for telling Anthropic to shut down Fable 5, its newest AI model, but there is some reality here. If the president wants the US to be the world leader in AI, shutting down the development of and use of our leading AI software is not the way to do that. Perhaps the administration will come to its senses, but in the

meantime, Anthropic has turned off its newest AI model. The administration says it is a national security issue, but just like the government's spectacularly failed attempt to kill off encryption in the 1990s, this is also doomed to fail. What the government did was issue an order saying that a license is required for each copy of Fable 5 which is used by someone outside the United States (an export) and also prohibits non US citizens from accessing Fable from inside the United States. This includes Anthropic employees, some of whom are Chinese and many of whom are outside the United States. If those people can't work on Anthropic software they will likely go to work (since they are outside the US) for companies in other countries (like China) that compete with our hoped-for dominance in AI. If this rule stands, it will give other countries the opportunity to catch up with and potentially surpass whatever AI leadership we have. This is a developing story, so stay tuned. If Anthropic wanted to continue allowing people to use Fable 5 they would need to do something like this. Obtain a copy of each individual user's passport, validate that it is a valid passport, figure out how to make sure that the person using it is the person whose passport they have, figure out a way to make sure that the named person was the only person using the account, etc.. All at scale and consider that half the US population doesn't even have a passport. Credit: [Gary Marcus](#)

CISA Issues BOD on Patching Because, Apparently, Agencies Don't Patch

The AI executive order (EO 14449) that the president signed required a bunch of agencies to generate a lot of paperwork. CISA is responding. Binding Operational Directive 26-04 requires all civilian executive branch agencies to patch their systems, prioritizing ones that have known exploited vulnerabilities and ones that are Internet facing. Apparently, you have to tell agencies to do that. That slam aside, the instructions are solid and if you are not doing this you should. They also, at the same time, released guidance. Hopefully, you won't find anything earth shaking in it, but you should check to see if it completely aligns with what you are doing. Now CISA can check the box that they met the requirements of the EO.

The BOD also lays out the timeline for agencies to deploy patches based on risk and you may not like those numbers. For high risk vulnerabilities, assess in 2-24 hours, patch in 3 days and in some cases, do forensics. If you are in a regulated industry, don't be surprised if regulators pile on and say those times should be your timeline too.

The BOD is [here](#) and the guidance is [here](#).

AI Alerts

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

Is Your AI Infrastructure Ready for AI in Production?

Maybe you have been testing AI and have built some agents. Maybe even your own LLM. But, the move from pilot to production is not easy. Your infrastructure probably is not set up for that; your disks are not fast enough; you don't have enough memory and maybe bandwidth. Definitely something to consider. The big folks (Amazon, Microsoft) are wrestling with this so don't think you won't also. If you are using the cloud for your AI deployment, make sure you understand how large your bill is going to be. If you need assistance, please contact us. Credit: [ITPro](#)

Claude Fable 5 - their most powerful model ever released to the public

Anthropic unveiled two new powerful AI models built on its previously restricted Mythos architecture: Claude Fable 5, which is being made broadly available, and Claude Mythos 5, which remains limited to a small group of cybersecurity and infrastructure partners.

Anthropic describes Fable 5 as the most capable model it has ever released to the public, outperforming previous Claude models across software engineering, scientific research, vision, and complex knowledge-work tasks. Anthropic says the model's advantage grows as tasks become longer and more complicated, enabling users to assign larger projects to the system with less oversight and fewer detailed instructions. [Details here](#)

Are AI agents the new weakest link in the security chain?

A phishing simulation on an OpenClaw email agent demonstrated it can be easily phished. This is all very immature technology, so we recommend being careful. It looks like the test that the researchers did was a reasonable model of the real world. Even in strict mode, it failed the phishing tests some of the time. This means that security permissions and access controls become even more important than they were before. If you need assistance, please contact us. 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.

Our MSP has one userid that they share across their techs. Is this okay?

The short answer is no. You have to be able to uniquely identify each person. If you can't do that, you are not compliant. Period.

Reference

Cyber Insurance Rates Down, but so is Coverage

Gartner says that while policy pricing has stabilized and carriers are providing discounts if you can DEMONSTRATE the right cyber hygiene, EXCLUSIONS are expanding. Among the most concerning exclusions are the security measures you SHOULD have in place. These include employee boo-boos, outdated software, poor security controls and mergers and acquisitions. These are just a few of the possible exclusions. If someone socially engineers your employee to send them a million dollars, that is not a CYBERcrime. While it is a crime, they didn't hack. They didn't take over your systems. They did not impersonate anyone. This is not a cybercrime. It is a failure of your controls. We can review your policy and also your security practices.

Credit: [Dark Reading](#)

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

Is this the new norm thanks to AI? Microsoft releases over 200 patches this week

Microsoft today released software updates to plug over 200 security holes across its Windows operating systems and supported software, a record number of fixes for the company's monthly

Patch Tuesday cycle. Nearly three dozen of those bugs earned Microsoft's most dire "critical" rating, and exploit code for at least three of the weaknesses is now publicly available.

Legislative and Legal Activities

Nothing to report

Education

Nothing to report

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.**

Oracle Warns of Bug That Hackers Used to Breach Over 100 Companies

Oracle warned customers about a critical vulnerability in PeopleSoft. Hacking group ShinyHunters claims to have breached more than a hundred organizations that use PeopleSoft. As of now, there is no patch available. ShinyHunters has published the hacked data of some of its attacks. Credit: [Tech Crunch](#)

OOPSIE. Japanese Energy Firm LOSES Drive with 10.9 Million Client's Data

Kyushu Electric Power announced that it lost (misplaced) a hard drive used for backups that, in theory, should have been locked in a server room protected by "multiple physical safeguards". But when they went to retrieve the drive, the locked cabinet was found unlocked and the drive was missing. Credit: [Bleeping Computer](#)

Prez says he is considering "investing" in AI companies

The president says he is considering "investing" in AI companies. Until this administration, other than the occasional fiscal bailout, the US government has not just bought an interest in companies. But part of the reason may be to bail out these companies. Some of them are hemorrhaging cash at an unsustainable rate. While state ownership in companies is common in communist countries like China, it is not common here - until recently. Whether that "investment" would include one or more board seats or what percentage ownership that might entail is still unknown. Learn more [here](#).

People becoming more thoughtful about AI

As people are beginning to realize that AI is not going away, people are starting to dig into some of the security and operational (privacy, for example) issues that come with AI. Where is my data? How is it being used? Does my data even stay in the US? If this is an area where you have more questions than answers, please reach out to us. Learn more [here](#).

UK tells big tech to block nudes - in 3 months

While the concept of protecting kids from bad stuff is a time honored political winner - sort of like politicians kissing babies - you do have to think things through. At this point the bill isn't even written. The government does say that 90 percent of the CSAM (aka kiddie porn) reports they received in 2024 had content that kids generated themselves. This requirement is not very easy

to implement for a variety of reasons such as shared computers and figuring out whether someone is, say, a 15 year old or a 17 year old (different rules). Learn more [here](#).

Security News for the week ending June 12, 2026

This week's news: EU turns to Russian alternative to Microsoft Office, former twitter engineer who warned about Grok's safety was fired and is now suing, Senate votes to not create new Pentagon branch, Cyber Force, feds shut down a couple of deep fake porn sites - call it groundbreaking and FISA section 702 lapses (lapsed) at Midnight (Friday). Details [here](#).

While CISA ordered agencies to get their patching act together, legally that does not apply to you. On the other hand, the advice is good but the time schedule is hard. You may see this in a regulation affecting you in the near future if you are in a regulated industry. If your patching hygiene is of concern, let us assist you in remedying that..

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663