

Mar 1, 2026

White House tries to get allies to use US AI stack but rejects global AI governance

It will be interesting to see if anyone bites. It is likely that small countries without any tech industry might, but without any governance rules, that might be a hard sell. The White House urged allies to ignore AI governance and use our stuff anyway. Obviously, the US tech industry loves the idea of selling our tech to other countries with no requirement to be responsible. Stay tuned. Credit: [Data Breach Today](#)

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

Attention Cisco Users - SD-WAN Zero-Day Exploited for Years

The Five-Eyes countries have issued an [EMERGENCY DIRECTIVE](#) saying that this vulnerability is being actively exploited to gain unauthorized access. [CISA issued its own order](#) to federal agencies. They only have until Friday evening to patch their stuff (that would be two days before this newsletter goes out). US agencies also have to scan their networks for signs of compromise after they deploy the patch. The bug, which is an authentication bypass, allows remote hackers to compromise controllers and add malicious rogue peers. It is scored as a **10.0**. You can't get higher than that. Even Cisco says the bug is being actively exploited. Credit: [Bleeping Computer](#)

AI Alerts

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

White House tries to get allies to use US AI stack but rejects global AI governance

It will be interesting to see if anyone bites. It is likely that small countries without any tech industry might, but without any governance rules, that might be a hard sell. The White House

urged allies to ignore AI governance and use our stuff anyway. Obviously, the US tech industry loves the idea of selling our tech to other countries with no requirement to be responsible. Stay tuned. Credit: [Data Breach Today](#)

Anthropic Tells Pentagon “NO”

This has never happened in history. The Pentagon wants Anthropic, maker of Claude AI, to remove safety guardrails so that they can surveil US citizens at will and use it to create fully automated weapons systems. Anthropic CEO Dario Amodei said no (until they say the technology is ready). If the government prevails, this would mean that no maker of an AI driven system would have any ability to control how it is used and could be dragged into a legal quagmire no matter whether they removed the guardrails or kept them in place. I assume Anthropic got board approval. Whatever Hegseth does, he will drag both the federal government and Anthropic into a legal fight that will make its way up to the Supreme Court. The Pentagon could axe them as a vendor, which is their right or they could designate them as a supply chain risk, something up until now which has been reserved for, say, Chinese companies - a threat to national security. Finally, they could (try to) invoke the Defense Production Act, saying that their particular AI is critical to national security and hence the government would want to force them to do something they don't want to do. It is hard to rationalize that they are both a supply chain risk and also at the same time critical to national security. Stay tuned. The ball is in Pentagon Pete's court. Credit: [Compliance Hub](#)

CMMC Q&A

I get to listen to hours and hours of webinars every week, so you don't have to. This week has a lot of CMMC information. If you have to comply, please contact us.

Q: Another DoD prime posts questionnaire to its vendors

A: This time it is Parsons, a publicly traded defense contractor focused on intelligence and infrastructure, based in Virginia. They are asking their subs to complete a questionnaire about where they stand with regard to CMMC compliance by March 3rd. I posted the entire questionnaire on the [CMMC requirements page](#); check out what specific questions they are asking.

Reference

Treasury Releases Resources on AI Use for Financial Sector

Just because you can do something does not mean it is approved in any regulated industry. The Treasury released two documents - an AI dictionary (lexicon) for people who don't understand the terms that AI uses, which includes a very brief explanation of those terms and a financial services AI risk management framework. While the financial sector is welcome to use this framework, there is no legal requirement to do so. There is a somewhat overt recommendation that you join the Cyber Risk Institute for an annual fee based on the size of your organization, but you do not have to. Credit: [US Department of the Treasury](#)

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

Nothing to report

Legislative and Legal Activities

Step Finance, SolanaFloor and Remora Markets Shut Down After Cyberattack

They lost \$30 million in a cyberattack in January and were unable to figure out how to recover the money, so they are shutting down immediately. I assume anyone who invested - or rather speculated - in their stuff is left holding the bag. Such is the nature of speculation. Credit: [Web 3 Is Going Great](#)

Education

Here is What a Google Subpoena Response Looks Like

Google says that they review subpoenas and sometimes push back but we rarely get to see what they actually look like. Courtesy of the Jeffrey Epstein Transparency Act, we are getting to see some of them. While they are supposed to be secret, they got dumped with millions of other documents recently. If you are curious about how these work, check this out. Credit: [DNYUZ](#)

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.

Scam? But there is a legitimate message

There is a report of an AI agent that meant to send \$4 to a beggar but, instead, sent his entire wallet. Is the story a scam? Possibly. Is it a promo for a new token? Maybe. But the message is that if you give your AI agent access to your money and there is a software error and you lose all of your crypto, you are on your own. US law won't give you back your money like in the case of credit card fraud. Just a word to the wise. Credit: [Cybernews](#)

US healthcare diagnostics firm hit by ransomware

Vikor Scientific, now called Vanta Diagnostics, announced a data breach affecting 140,000 people. The hackers have published the stolen data. Not surprisingly, the data stolen was data they shared with a third party business partner. Credit: [Security Week](#)

CarGurus Breach Exposes 12 Million Accounts

CarGurus gets 40 million car enthusiasts a month visiting their website. Information exposed when the hackers published the data includes email, name, phone, physical address, finance application data and outcomes and other information. Credit: [Bleeping Computer](#)

AI for good - cybersecurity good

This time it is both good and bad. A Russian hacker breached 600 firewalls just using a couple of off the shelf AI tools. Note this wasn't rocket science - these were poorly protected firewalls. But AI also found over 500 vulnerabilities in open source code bases that were publicly available and now you, too, can use this tool to find vulnerabilities in your code. Learn more [here](#).

Cyber growth constrained by physical limits

This is not what you usually think of when we talk about the limits of AI, but it is real. The time to get building permits, the lack of workers as a result of the president's deportation efforts and the lack of electric power. Experts say that 30 to 50 percent of new data centers will be late. Learn more [here](#).

When AI becomes the weapon

Another single hacker (this is not the story above), two AI tools and nine agencies get compromised and 150 gigabytes of personal information is stolen. This is only the beginning of AI wonderfulness. Learn more [here](#).

Security News for the week ending February 27, 2026

This week's news: are Waymo and Tesla's driverless cars really driverless, latest delivery scam - fake carriers calling you to return your phone, a simple solution to illegal immigration blocked by red states, Anthropic tells DoD no; OpenAI says yes and CISA replaces one placeholder leader with another placeholder. Details [here](#).

We are seeing more AI driven cyber attacks every week. If you are still protecting your network the same way you did two or three years ago, you will not be able to keep up with AI driven attacks. Please contact us if you need an assessment or assistance.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663