

September 13, 2026

Treasury to Help Financial Firms Transition to Quantum Resistant Encryption

The Treasury's concern is that once quantum computers are available, all historical and future financial transactions are at risk of decryption, threat and use in attacks. Given that the government would prefer the financial system does not collapse, they, kind of, have a dog in the fight. What are they doing? Well, of course, they formed a task force. It is not clear WHO they will work with and WHAT they will provide. Details are to be determined. Credit: [Cybersecurity Dive](#)

Please check out our blog at [HTTPS://TCPS-BLOG.COM](https://TCPS-BLOG.COM)

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

Microsoft's Best Friend (or Worst Enemy) Released Another Defender 0-Day

The researcher, known as NIGHTMARE ECLIPSE, released another Microsoft Defender zero-day including a bare bones proof of concept. This one is called Shield Crash, which bypasses the patch for ShieldBreak and allows the attacker to read system files. He said he was feeling lazy so he did not enhance the proof of concept into a full system compromise, but he might later. Microsoft, it is time to kiss and make up. This is his eleventh Microsoft zero-day/. Credit: [The Register](#)

AI Alerts

Check out our Certified AI Governance Leader Course at [AIGIP.AI](#). If you are a government employee, check out our AI Governance for Govies at the same site.

Want to stay on top of the news about AI - Check out our news feed on the AIGIP web site at <https://aigip.ai/news/latest-ai-news>

Anthropic is Working Hard to Keep Up With OpenAI

Each of them have a felony count of at least four right now. At least, that is all they have admitted to. [Felony Bench](#) is tracking these felonies. Actually, according to the web site, the count is much higher. Maybe the folks that think AI will kill us all are right. Credit: [The Register](#)

OpenAI Promises to Spend \$1 Billion on Protecting Critical Infrastructure (Sort of)

What they are promising is to give away some of their software to small water and electric utilities to help them protect themselves. Well, actually, they are just subsidizing the cost of their software, so this is really a sales technique. They are also subsidizing the cost of training and technical support. For utilities that maybe, have a single IT person, who likely has other jobs, it is unclear that this is helpful. It is a great PR move, but unlikely to make much of a difference since these utilities don't have the resources to use the tools. Credit: [CSO Online](#)

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.*

The 60 Day Review Timeline is Over - Now What?

Just to be clear. There are no requirements around the 60 days at all. The task force was created by a memo from Kirsten (DoD CIO), not Congress. We might see something at some time. We might not. She said she was going to make something public so she might. No requirement. And, the pause of Phase 2 was implemented by a different mechanism, so that goes on until the waiver or class deviation, whatever they did, is rescinded.

How Does the FAR CUI Rule Affect CMMC?

The answer is no one knows but the FAR CUI rule does apply to defense contractors if and when it is released. COULD DoD CIO Davies say that CMMC is going away and we are going to make the protection of CUI the GSA's problem. She could - probably not without so much blowback that it won't happen. So, in the very unlikely case that this is her strategy to make it someone else's problem, what does this mean? First of all, it takes effect as soon as it is published. There is no 4-7 year ramp time like there is with CMMC. Second, it requires compliance with 800-171 Rev 3 - immediately. And other things. For example, for CMMC there is a scoping guide; that doesn't exist for the FAR CUI rule, so at least at the moment, everything is in scope. And, as I said, no phase in. Be careful what you wish for.

**** REMINDER** NEW SPRS/PIEE System Access Requirements**

This is not a change to CMMC, but PIEE is now requiring that you log in at least every 34 days to keep your account active, so make sure you put this on your recurring task list.

Reference

Treasury to Help Financial Firms Transition to Quantum Resistant Encryption

The Treasury's concern is that once quantum computers are available, all historical and future financial transactions are at risk of decryption, threat and use in attacks. Given that the government would prefer the financial system does not collapse, they, kind of, have a dog in the fight. What are they doing? Well, of course, they formed a task force. It is not clear WHO they

will work with and WHAT they will provide. Details are to be determined. Credit: [Cybersecurity Dive](#)

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

Router Maker MikroTik Patches Bugs Currently Being Exploited

The attack named MikroTrick chains two bugs together to obtain root access with routers that have SSH exposed to the Internet. There are at least 120,000 of them. MikroTik has released patches to six bugs. Credit: [CSO Online](#)

Legislative and Legal Activities

Musk's xAI Fails to Block Minnesota Law Banning Nudification Apps

Minnesota's law banning platforms from hosting AI tools that create nonconsensual fake nude images became enforceable last month. The law has fines of up to \$500,000 per unlawful use. Musk wanted a stay on the law until he exhausted efforts to overturn it. The judge says the public interest favored Minnesota. Nudification apps are the current version of kiddie porn - they serve no ethical purpose and harm people. Musk doesn't want to be constrained, especially if it could cost him a lot of money. When Twitter first started offering nudification apps, they generated over a million visits in the first 3 or 4 months. Multiple that by \$500,000 per visit and that is about \$500 billion in potential liability in that short time span. While the law doesn't make him liable for past visits, it could make him liable for future ones if he doesn't stop them. On the other hand, they may generate significant advertising revenue. Money talks - in both directions. Credit: [Cybernews](#)

Canada is Fast Tracking a Bill to Force US companies to Secretly Spy on Americans

The bill, called the Lawful Access Act, is similar to bills in many other countries and is designed to try and force tech companies (US and others) to provide surveillance data to Canadian authorities, secretly. This could include both forcing companies to store metadata and even add, secretly, back doors that compromise the security of their software. This is sort of related to the US CLOUD act, but extends the surveillance even further. This could put tech companies in a bind between breaking US law and breaking Canadian law. It would allow, taken to extreme, the Canadian government to force US tech companies to spy on US Senators and Cabinet officials, all secretly. Credit: [The Record](#)

KIDS Act Passes the House; Odds Uncertain in the Senate

A requirement for tech companies to operate under a "duty of care" is gone, but age verification of some web sites is still there (even though we just had a breach of 150 million IDs, which would be mandated under this bill), a ban on private messaging by kids under 13 (unenforceable), a prohibition on disappearing messages for kids under 17 (likewise unenforceable), rules about interacting with chatbots, etc. Hopefully the Senate will realize that Senator's privacy will be eliminated by this bill and reject it. Credit: [My Privacy Blog](#)

Education

EU's Cyber Resilience Act Goes Into Effect - A Game of Cyber Chicken

The CRA, among other things, gives software makers a VERY short fuse for reporting vulnerabilities to the EU government. If you are completely based in the US then the EU is unlikely to sue you if you fail to report, but they do have another stick - tell EU ISPs to block your domain. If you don't sell to EU entities you don't care, but if you have customers in the EU, that would be a problem. Read this [report](#) to learn about the new reporting requirement.

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.

OpenAI Agents Hijack Another Victim

OpenAI agents made more than 15,000 edits to a German Wiki over three months. The obvious message here is that the security controls we used up until now will not protect us from AI, but if you think they will, we wish you the best of luck. Credit: [Security Week](#)

Why the 'Bigbear' Phishing Attack Should be on Your Radar

The attack allows attackers to bypass your MFA that you thought keeps you safe. Already 250 organizations and 5,000 user accounts have been compromised and the attack is not that sophisticated. Learn how it works [here](#).

And the Winner is ... Microsoft With 974+ Patches

That does qualify for a record for Microsoft. It is their single biggest patch release in the history of the company. What they didn't say is how many bugs they discovered. That may be significantly larger than the number that they patched. Learn more [here](#).

New State Cloud Rules Will Impact Vendors

For vendors who sell to the public sector there are new rules in multiple states. In several states you may need to be FedRAMP/StateRAMP certified in order to sell. If you have questions about this, please contact us. Learn more [here](#).

Security News for the week ending September 11, 2026

This week's news: UK Online Safety Act has made "ABSOLUTELY NO DIFFERENCE", kids say, Want to tell Zuck to ZuckOff - you can if you are an iPhone user, RAND says we could not replace satellites destroyed in case of a war, the government lacks the ability to verify AI companies' claims and EU says Google must open up Gemini and search to competitors. Learn more [here](#).

The cyber threat is growing at an amazing clip with AI being a key factor. If your cybersecurity program is still based on a reality of just two years ago, you are looking for problems. Contact us if you need to upgrade your program.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663

