KrebsonSecurity
In-depth security news and investigation

A Tumultuous Week for Federal Cybersecurity Efforts

January 27, 2025 114 Comments

Image: Shutterstock. Greg Meland.

President Trump last week issued a flurry of executive orders that upended a number of government initiatives focused on improving the nation's cybersecurity posture. The president fired all advisors from the Department of Homeland Security's Cyber Safety Review Board, called for the creation of a strategic cryptocurrency reserve, and voided a Biden administration action that sought to reduce the risks that artificial intelligence poses to consumers, workers and national security.

On his first full day back in the White House, Trump dismissed all 15 advisory committee members of the Cyber Safety Review Board (CSRB), a nonpartisan government entity established in February 2022 with a mandate to investigate the causes of major cybersecurity events. The CSRB has so far produced three detailed reports, including an analysis of the Log4Shell vulnerability crisis, attacks from the cybercrime group LAPSUS$, and the 2023 Microsoft Exchange Online breach.

The CSRB was in the midst of an inquiry into cyber intrusions uncovered recently across a broad spectrum of U.S. telecommunications providers at the hands of Chinese state-sponsored hackers. One of the CSRB's most recognizable names is **Chris Krebs** (no relation), the former director of the **Cybersecurity and Infrastructure Security Agency** (CISA). Krebs was fired by President Trump in November 2020 for declaring the presidential contest was the most secure in American history, and for refuting Trump's false claims of election fraud.

South Dakota Governor **Kristi Noem**, confirmed by the U.S. Senate last week as the new director of the DHS, criticized CISA at her confirmation hearing, *TheRecord* reports.

Noem told lawmakers CISA needs to be "much more effective, smaller, more nimble, to really fulfill their mission," which she said should be focused on hardening federal IT systems and hunting for digital intruders. Noem said the agency's work on fighting misinformation shows it has "gotten far off mission" and involved "using their resources in ways that was never intended."

"The misinformation and disinformation that they have stuck their toe into and meddled with, should be refocused back onto what their job is," she said.

Moses Frost, a cybersecurity instructor with the SANS Institute, compared the sacking of the CSRB members to firing all of the experts at the **National Transportation Safety Board** (NTSB) while they're in the middle of an investigation into a string of airline disasters.

"I don't recall seeing an 'NTSB Board' being fired during the middle of a plane crash investigation," Frost said in a recent SANS newsletter. "I can say that the attackers in the phone companies will not stop because the review board has gone away. We do need to figure out how these attacks occurred, and CISA did appear to be doing some good for the vast majority of the federal systems."

Speaking of transportation, *The Record* notes that Transportation Security Administration chief **David Pekoske** was fired despite overseeing critical cybersecurity improvements across pipeline, rail and aviation sectors. Pekoske was appointed by Trump in 2017 and had his 5-year tenure renewed in 2022 by former President Joe Biden.

AI & CRYPTOCURRENCY

Shortly after being sworn in for a second time, Trump voided a Biden executive order that focused on supporting research and development in artificial intelligence. The previous administration's order on AI was crafted with an eye toward managing the safety and security risks introduced by the technology. But a statement released by the White House said Biden's approach to AI had hindered development, and that the United States would support AI systems that are "free from ideological bias or engineered social agendas," to maintain leadership.

The Trump administration issued its own executive order on AI, which calls for an "AI Action Plan" to be led by the assistant to the president for science and technology, the White House "AI & crypto czar," and the national security advisor. It also directs the White House to revise and reissue policies to federal agencies on the government's acquisition and governance of AI "to ensure that harmful barriers to America's AI leadership are eliminated."

Trump's AI & crypto czar is **David Sacks**, an entrepreneur and Silicon Valley venture capitalist who argues that the Biden administration's approach to AI and cryptocurrency has driven innovation overseas. Sacks recently asserted that non-fungible cryptocurrency tokens and memecoins are neither securities nor commodities, but rather should be treated as "collectibles" like baseball cards and stamps.

There is already a legal definition of collectibles under the U.S. tax code that applies to things like art or antiques, which can be subject to high capital gains taxes. But **Joe Hall**, a capital markets attorney and partner at Davis Polk, told *Fortune* there are no market regulations that apply to collectibles under U.S. securities law. Hall said Sacks' comments "suggest a viewpoint that it would not be appropriate to regulate these things the way we regulate securities."

The new administration's position makes sense considering that the Trump family is deeply and personally invested in a number of recent memecoin ventures that have attracted billions from investors. President Trump and First Lady Melania Trump each launched their own vanity memecoins this month, dubbed **$TRUMP** and **$MELANIA**.

The Wall Street Journal reported Thursday the market capitalization of $TRUMP stood at about $7 billion, down from a peak of near $15 billion, while $MELANIA is hovering somewhere in the $460 million mark. Just two months before the 2024 election, Trump's three sons debuted a cryptocurrency token called **World Liberty Financial**.

Despite maintaining a considerable personal stake in how cryptocurrency is regulated, Trump issued an executive order on January 23 calling for a working group to be chaired by Sacks that would develop "a federal regulatory framework governing digital assets, including stablecoins," and evaluate the creation of a "strategic national digital assets stockpile."

Translation: Using taxpayer dollars to prop up the speculative, volatile, and highly risky cryptocurrency industry, which has been marked by endless scams, rug-pulls, 8-figure cyber heists, rampant fraud, and unrestrained innovations in money laundering.

WEAPONIZATION & DISINFORMATION

Prior to the election, President Trump frequently vowed to use a second term to exact retribution against his perceived enemies. Part of that promise materialized in an executive order Trump issued last week titled "Ending the Weaponization of the Federal Government," which decried "an unprecedented, third-world weaponization of prosecutorial power to upend the democratic process," in the prosecution of more than 1,500 people who invaded the U.S. Capitol on Jan. 6, 2021.

On Jan. 21, Trump commuted the sentences of several leaders of the Proud Boys and Oath Keepers who were convicted of seditious conspiracy. He also issued "a full, complete and unconditional pardon to all other individuals convicted of offenses related to events that occurred at or near the United States Capitol on January 6, 2021," which include those who assaulted law enforcement officers.

The New York Times reports "the language of the document suggests — but does not explicitly state — that the Trump administration review will examine the actions of local district attorneys or state officials, such as the district attorneys in Manhattan or Fulton County, Ga., or the New York attorney general, all of whom filed cases against President Trump."

Another Trump order called "Restoring Freedom of Speech and Ending Federal Censorship" asserts:

"Over the last 4 years, the previous administration trampled free speech rights by censoring Americans' speech on online platforms, often by exerting substantial coercive pressure on third parties, such as social media companies, to moderate, deplatform, or otherwise suppress speech that the Federal Government did not approve," the Trump administration alleged. "Under the guise of combatting 'misinformation,' 'disinformation,' and 'malinformation,' the Federal Government infringed on the constitutionally protected speech rights of American citizens across the United States in a manner that advanced the Government's preferred narrative about significant matters of public debate."

Both of these executive orders have potential implications for security, privacy and civil liberties activists who have sought to track conspiracy theories and raise awareness about disinformation efforts on social media coming from U.S. adversaries.

In the wake of the 2020 election, Republicans created the **House Judiciary Committee's Select Subcommittee on the Weaponization of the Federal Government**. Led by GOP **Rep. Jim Jordan** of Ohio, the committee's stated purpose was to investigate alleged collusion between the Biden administration and tech companies to unconstitutionally shut down political speech.

The GOP committee focused much of its ire at members of the short-lived Disinformation Governance Board, an advisory board to DHS created in 2022 (the "combating misinformation, disinformation, and malinformation" quote from Trump's executive order is a reference to the board's stated mission). Conservative groups seized on social media posts made by the director

of the board, who resigned after facing death threats. The board was dissolved by DHS soon after.

In his first administration, President Trump created a special prosecutor to probe the origins of the FBI's investigation into possible collusion between the Trump campaign and Russian operatives seeking to influence the 2016 election. Part of that inquiry examined evidence gathered by some of the world's most renowned cybersecurity experts who identified frequent and unexplained communications between an email server used by the **Trump Organization** and **Alfa Bank**, one of Russia's largest financial institutions.

Trump's Special Prosecutor **John Durham** later subpoenaed and/or deposed dozens of security experts who'd collected, viewed or merely commented on the data. Similar harassment and deposition demands would come from lawyers for Alfa Bank. Durham ultimately indicted **Michael Sussman**, the former federal cybercrime prosecutor who reported the oddity to the FBI. Sussman was acquitted in May 2022. Last week, Trump appointed Durham to lead the U.S. attorney's office in Brooklyn, NY.

Quinta Jurecic at *Lawfare* notes that while the executive actions are ominous, they are also vague, and could conceivably generate either a campaign of retaliation, or nothing at all.

"The two orders establish that there will be investigations but leave open the questions of what kind of investigations, what will be investigated, how long this will take, and what the consequences might be," Jurecic wrote. "It is difficult to draw firm conclusions as to what to expect. Whether this ambiguity is intentional or the result of sloppiness or disagreement within Trump's team, it has at least one immediate advantage as far as the president is concerned: generating fear among the broad universe of potential subjects of those investigations."

On Friday, Trump moved to fire at least 17 inspectors general, the government watchdogs who conduct audits and investigations of executive branch actions, and who often uncover instances of government waste, fraud and abuse. Lawfare's **Jack Goldsmith** argues that the removals are probably legal even though Trump defied a 2022 law that required congressional notice of the terminations, which Trump did not give.

"Trump probably acted lawfully, I think, because the notice requirement is probably unconstitutional," Goldsmith wrote. "The real bite in the 2022 law, however, comes in the limitations it places on Trump's power *to replace* the terminated IGs—limitations that I believe are constitutional. This aspect of the law will make it hard, but not impossible, for Trump to put loyalists atop the dozens of vacant IG offices around the executive branch. The ultimate fate of IG independence during Trump 2.0, however, depends less on legal protections than on whether Congress, which traditionally protects IGs, stands up for them now. Don't hold your breath."

Among the many Biden administration executive orders revoked by President Trump last week was an action from December 2021 establishing the **United States Council on Transnational Organized Crime**, which is charged with advising the White House on a range of criminal activities, including drug and weapons trafficking, migrant smuggling, human trafficking,

cybercrime, intellectual property theft, money laundering, wildlife and timber trafficking, illegal fishing, and illegal mining.

So far, the White House doesn't appear to have revoked an executive order that former President Biden issued less than a week before President Trump took office. On Jan. 16, 2025, Biden released a directive that focused on improving the security of federal agencies and contractors, and giving the government more power to sanction the hackers who target critical infrastructure.

This entry was posted on Monday 27th of January 2025 09:50 PM

A LITTLE SUNSHINE THE COMING STORM

ALFA BANK DAVID SACKS HOUSE JUDICIARY COMMITTEE'S SELECT SUBCOMMITTEE ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT JACK GOLDSMITH JOE HALL JOHN DURHAM LAWFARE MELANIA TRUMP MICHAEL SUSSMAN PRESIDENT TRUMP QUINTA JURECIC REP. JIM JORDAN UNITED STATES COUNCIL ON TRANSNATIONAL ORGANIZED CRIME WORLD LIBERTY FINANCIAL

114 thoughts on "A Tumultuous Week for Federal Cybersecurity Efforts"

Donna

January 28, 2025

Thank you for this excellent recap, Brian. I truly appreciate how you've pulled together the facts and provided links to help us look back over this past week's actions.

Lou

-

January 29, 2025

agree !

mark

January 28, 2025

And… he shut all this down, just as he launched his own cryptocurrency, *and* China, suspected of the telecom hack, and announced their own, better, AI.

Sold to the highest bidder?

ctar

January 28, 2025

These comments are all over the place. Can someone clarify for me whether this article is left leaning or right leaning? Pro Trump or anti Trump? Is there malicious intent in the presentation of the information that I am just not smart enough to see? Thank you in advance.

AK

-

January 28, 2025