



Trump 2.0 Brings Cuts to Cyber, Consumer Protections

February 23, 2025

100 Comments

One month into his second term, President Trump's actions to shrink the government through mass layoffs, firings and withholding funds allocated by Congress have thrown federal cybersecurity and consumer protection programs into disarray. At the same time, agencies are battling an ongoing effort by the world's richest man to wrest control over their networks and data.



Image: Shutterstock. Greg Meland.

The Trump administration has fired at least 130 employees at the federal government's foremost cybersecurity body — the **Cybersecurity and Infrastructure Security Agency (CISA)**. Those dismissals **reportedly** included CISA staff dedicated to securing U.S. elections, and fighting misinformation and foreign influence operations.

Earlier this week, technologists with Elon Musk's **Department of Government Efficiency (DOGE)** **arrived at CISA** and gained access to the agency's email and networked files. Those DOGE staffers include **Edward "Big Balls" Coristine**, a **19-year-old former denizen of the "Com,"** an archipelago of Discord and Telegram chat channels that function as a kind of distributed **cybercriminal social network**.

The investigative journalist **Jacob Silverman** **writes** that Coristine is the grandson of **Valery Martynov**, a KGB double agent who spied for the United States. Silverman recounted how Martynov's wife **Natalya Martynova** moved to the United States with her two children after her husband's death.

"Her son became a Virginia police officer who sometimes posts comments on blogs about his historically famous father," Silverman wrote. "Her daughter became a financial professional who married Charles Coristine, the proprietor of LesserEvil, a snack company. Among their children is a 19-year-old young man named Edward Coristine, who currently wields an unknown amount of power and authority over the inner-workings of our federal government."

Another member of DOGE is **Christopher Stanley**, formerly senior director for security engineering at X and principal security engineer at Musk's **SpaceX**. Stanley, 33, had a brush with celebrity on Twitter in 2015 when he leaked the user database for the DDoS-for-hire service **LizardStresser**, and soon faced threats of physical violence against his family.

My **2015 story on that leak** did not name Stanley, but he exposed himself as the source by posting a video about it on his Youtube channel. A review of domain names registered by Stanley shows he went by the nickname "enKrypt," and was the former owner of a pirated software and hacking forum called **error33[.]net**, as well as **theC0re**, a video game cheating community.

"A NATIONAL CYBERATTACK"

DOGE has been steadily gaining sensitive network access to federal agencies that hold a staggering amount of personal and financial information on Americans, including the **Social Security Administration (SSA)**, the **Department of Homeland Security**, the **Office of Personnel Management (OPM)**, and the **Treasury Department**.

Most recently, DOGE has sought broad access to systems at the **Internal Revenue Service** that contain the personal tax information on millions of Americans, including how much individuals earn and owe, property information, and even details related to child custody agreements. The New York Times **reported Friday** that the IRS had reached an agreement whereby a single DOGE employee — 25-year-old **Gavin Kliger** — will be allowed to see only anonymized taxpayer information.

The rapidity with which DOGE has rifled through one federal database after another in the name of unearthing "massive fraud" by government agencies has alarmed many security experts, who warned that DOGE's actions bypassed essential safeguards and security measures.

"The most alarming aspect isn't just the access being granted," **wrote Bruce Schneier and David Ottenheimer**, referring to DOGE as a national cyberattack. "It's the systematic dismantling of security measures that would detect and prevent misuse—including standard incident response protocols, auditing, and change-tracking mechanisms—by removing the career officials in charge of those security measures and replacing them with inexperienced operators."

Jacob Williams is a former hacker with the **U.S. National Security Agency** who now works as managing director of the cybersecurity firm **Hunter Labs**. Williams kicked a virtual hornet's nest last week when he posted on LinkedIn that the network incursions by DOGE were "a bigger threat to U.S. federal government information systems than China."

Williams said while he doesn't believe anyone at DOGE would intentionally harm the integrity and availability of these systems, it's widely reported (and not denied) that DOGE introduced code changes into multiple federal IT systems. These code changes, he maintained, are not following the normal process for vetting and review given to federal government IT systems.

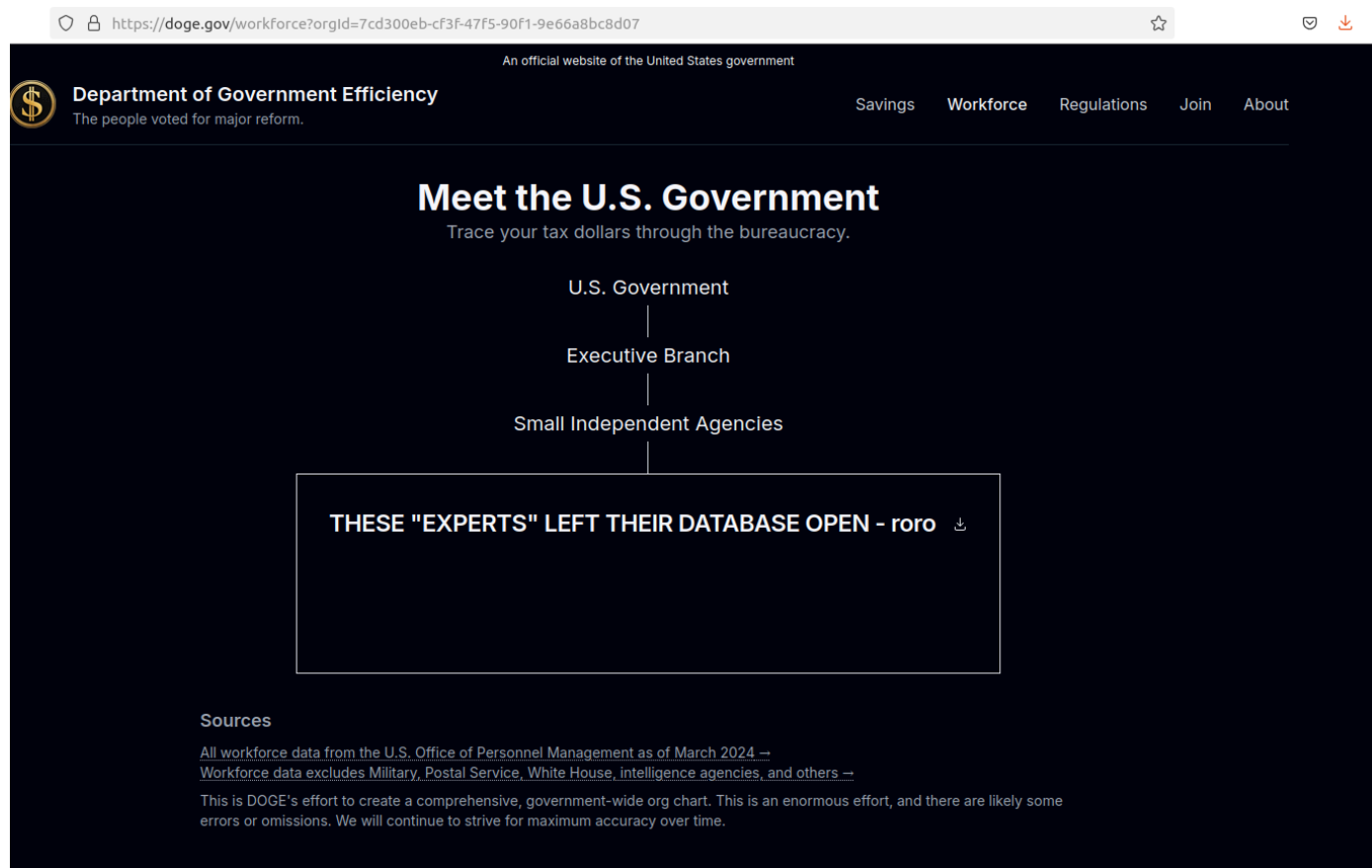
“For those thinking ‘I’m glad they aren’t following the normal federal government IT processes, those are too burdensome’ I get where you’re coming from,” Williams **wrote**. “But another name for ‘red tape’ are ‘controls.’ If you’re comfortable bypassing controls for the advancement of your agenda, I have questions – mostly about whether you do this in your day job too. Please tag your employer letting them know your position when you comment that controls aren’t important (doubly so if you work in cybersecurity). All satire aside, if you’re comfortable abandoning controls for expediency, I implore you to decide where the line is that you won’t cross in that regard.”

The DOGE website’s “wall of receipts” boasts that Musk and his team have saved the federal government more than \$55 billion through staff reductions, lease cancellations and terminated contracts. But a team of reporters at **The New York Times** found the math that could back up those checks is marred with accounting errors, incorrect assumptions, outdated data and other mistakes.

For example, DOGE claimed it saved \$8 billion in one contract, when the total amount was actually \$8 million, The Times found.

“Some contracts the group claims credit for were double- or triple-counted,” reads **a Times story with six bylines**. “Another initially contained an error that inflated the totals by billions of dollars. While the DOGE team has surely cut some number of billions of dollars, its slapdash accounting adds to a pattern of recklessness by the group, which has recently gained access to sensitive government payment systems.”

So far, the DOGE website does not inspire confidence: We learned last week that the doge.gov administrators somehow left their database wide open, allowing someone to publish messages that **ridiculed the site’s insecurity**.



A screenshot of the DOGE website after it was defaced with the message: "These 'experts' left their database open – roro"

APPOINTMENTS

Trump's efforts to grab federal agencies by their data has seen him replace career civil servants who refused to allow DOGE access to agency networks. **CNN reports** that **Michelle King**, acting commissioner of the Social Security Administration for more than 30 years, was shown the door after she denied DOGE access to sensitive information.

King was replaced by **Leland Dudek**, formerly a senior advisor in the SSA's Office of Program Integrity. This week, Dudek posted a now-deleted message on LinkedIn acknowledging he had been placed on administrative leave for cooperating with DOGE.

"I confess," Dudek wrote. "I bullied agency executives, shared executive contact information, and circumvented the chain of command to connect DOGE with the people who get stuff done. I confess. I asked where the fat was and is in our contracts so we can make the right tough choices."



Dudek's message on LinkedIn.

According to Wired, the **National Institute of Standards and Technology** (NIST) was also bracing this week for roughly 500 staffers to be fired, which could have serious impacts on NIST's cybersecurity standards and software vulnerability tracking work.

"And cuts last week at the US Digital Service included the cybersecurity lead for the central Veterans Affairs portal, VA.gov, potentially leaving VA systems and data more vulnerable without someone in his role," Wired's Andy Greenberg and Lily Hay Newman **wrote**.

NextGov **reports** that Trump named the Department of Defense's new chief information security officer: **Katie Arrington**, a former South Carolina state lawmaker who helped steer Pentagon cybersecurity contracting policy before being put on leave amid accusations that she disclosed classified data from a military intelligence agency.

NextGov notes that the **National Security Agency** suspended her clearance in 2021, although the exact reasons that led to the suspension and her subsequent leave were classified. Arrington

argued that the suspension was a politically motivated effort to silence her.

Trump also appointed the former chief operating officer of the **Republican National Committee** as the new head of the Office of National Cyber Director. **Sean Cairncross**, who has no formal experience in technology or security, will be responsible for coordinating national cybersecurity policy, advising the president on cyber threats, and ensuring a unified federal response to emerging cyber-risks, Politico [writes](#).

DarkReading [reports](#) that Cairncross would share responsibility for advising the president on cyber matters, along with the director of cyber at the White House National Security Council (NSC) — a group that advises the president on all matters security related, and not just cyber.

CONSUMER PROTECTION?

The president also ordered staffers at the **Consumer Financial Protection Bureau** (CFPB) to stop most work. Created by Congress in 2011 to be a clearinghouse of consumer complaints, the CFPB has sued some of the nation's largest financial institutions for violating consumer protection laws.

The CFPB says its actions have put nearly \$18 billion back in Americans' pockets in the form of monetary compensation or canceled debts, and imposed \$4 billion in civil money penalties against violators. The CFPB's homepage has featured a "404: Page not found" error for weeks now.

Trump has appointed **Russell Vought**, the architect of the conservative policy playbook **Project 2025**, to be the CFPB's acting director. Vought has publicly favored abolishing the agency, as has Elon Musk, whose efforts to remake X into a payments platform would otherwise be regulated by the CFPB.

The New York Times recently published a useful graphic showing all of the government staffing changes, including the firing of several top officials, affecting agencies with federal investigations into or regulatory battles with Musk's companies. Democrats on the House Judiciary Committee also have released [a comprehensive account \(PDF\)](#) of Musk's various conflicts of interest.

Trump firings hit agencies with oversight of Musk's companies

Staffing changes, including the firing of several top officials, have affected agencies with **federal investigations** into or **regulatory battles** with Elon Musk's companies.

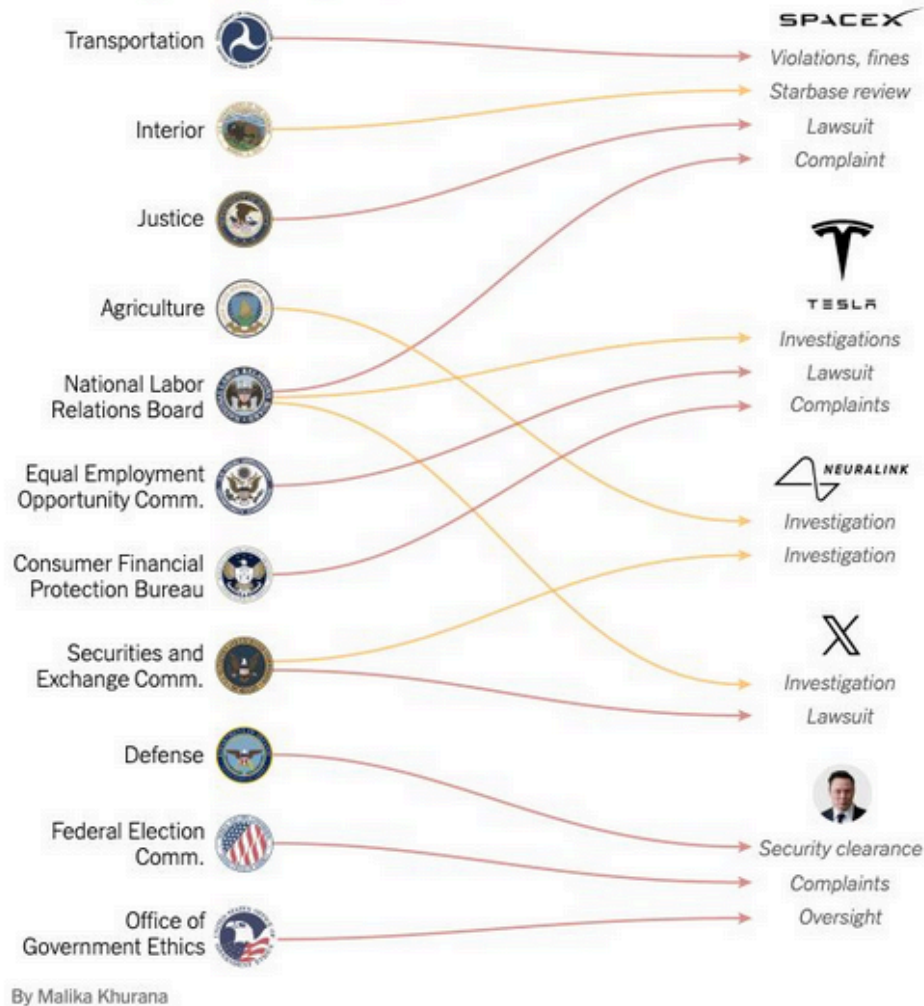


Image: nytimes.com

As the Times notes, Musk and his companies have repeatedly failed to comply with federal reporting protocols aimed at protecting state secrets, and these failures have prompted at least three federal reviews. Those include an inquiry launched last year by the Defense Department's Office of Inspector General. Four days after taking office, Trump fired the DoD inspector general along with 17 other inspectors general.

The Trump administration also shifted the enforcement priorities of the **U.S. Securities and Exchange Commission** (SEC) away from prosecuting misconduct in the cryptocurrency sector, reassigning lawyers and **renaming the unit** to focus more on "cyber and emerging technologies."

Reuters **reports** that the former SEC chair **Gary Gensler** made fighting misconduct in a sector he termed the "wild west" a priority for the agency, targeting not only cryptocurrency fraudsters but also the large firms that facilitate trading such as **Coinbase**.

On Friday, Coinbase said the SEC planned to withdraw its lawsuit against the crypto exchange. Also on Friday, the cryptocurrency exchange **Bybit** announced on X that a cybersecurity breach led to the theft of more than \$1.4 billion worth of cryptocurrencies — making it the largest crypto heist ever.

ORGANIZED CRIME AND CORRUPTION

On Feb. 10, Trump **ordered** executive branch agencies to stop enforcing the **U.S. Foreign Corrupt Practices Act**, which froze foreign bribery investigations, and even allows for “remedial actions” of past enforcement actions deemed “inappropriate.”

Trump’s action also disbanded the **Kleptocracy Asset Recovery Initiative** and **KleptoCapture Task Force** — units which proved their value in corruption cases and in seizing the assets of sanctioned Russian oligarchs — and diverted resources away from investigating white-collar crime.

That’s according to the independent **Organized Crime and Corruption Reporting Project** (OCCRP), an investigative journalism outlet that until very recently was funded in part by the **U.S. Agency for International Development** (USAID).

The **OCCRP** lost nearly a third of its funding and was forced to lay off 43 reporters and staff after Trump moved to shutter USAID and freeze its spending. NBC News **reports** the Trump administration plans to gut the agency and leave fewer than 300 staffers on the job out of the current 8,000 direct hires and contractors.

The **Global Investigative Journalism Network** **wrote** this week that the sudden hold on USAID foreign assistance funding has frozen an estimated \$268 million in agreed grants for independent media and the free flow of information in more than 30 countries — including several under repressive regimes.

Elon Musk has called USAID “a criminal organization” without evidence, and **promoted fringe theories** on his social media platform X that the agency operated without oversight and was rife with fraud. Just months before the election, USAID’s Office of Inspector General **announced** an investigation into USAID’s oversight of Starlink satellite terminals provided to the government of Ukraine.

KrebsOnSecurity this week heard from a trusted source that all outgoing email from USAID now carries a notation of “**sensitive but unclassified**,” a designation that experts say could make it more difficult for journalists and others to obtain USAID email records under the Freedom of Information Act (FOIA). On Feb. 20, Fedscoop **reported** also hearing the same thing from multiple sources, noting that the added message cannot be seen by senders until after the email is sent.

FIVE BULLETS

On Feb. 18, Trump issued **an executive order** declaring that only the U.S. attorney general and the president can provide authoritative interpretations of the law for the executive branch, and that this authority extends to independent agencies operating under the executive branch.

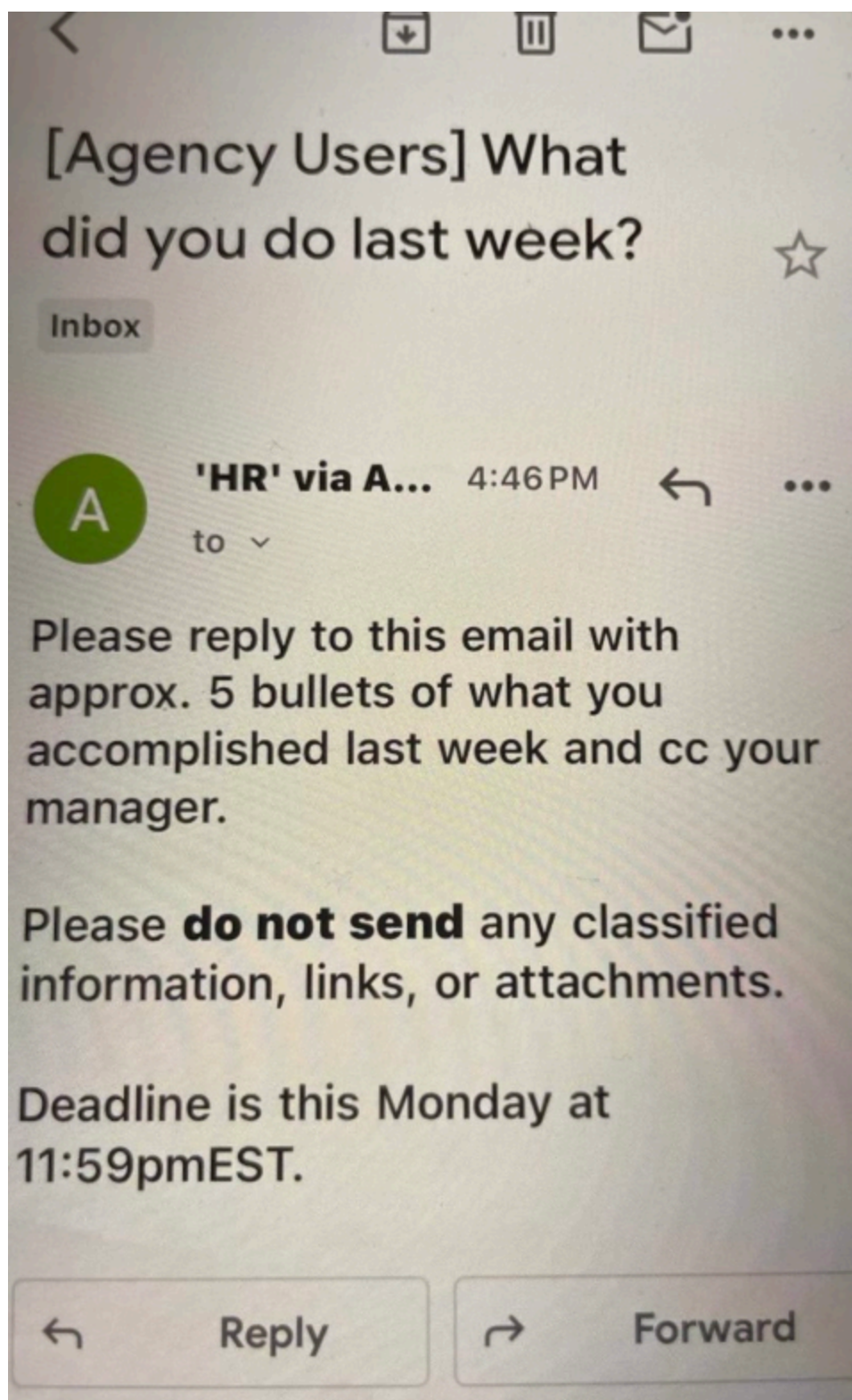
Trump is arguing that Article II, Clause 1 of the Constitution vests this power with the president. However, jurist.org **writes** that Article II does not expressly state the president or any other person in the executive branch has the power to interpret laws.

“The article states that the president is required to ‘take care that the laws be faithfully executed,’” Juris noted. “Jurisdiction to interpret laws and determine constitutionality belongs to the judicial branch under Article III. The framers of the Constitution designed the separation of duties to prevent any single branch of government from becoming too powerful.”

The executive order requires all agencies to submit to “performance standards and management objectives” to be established by the White House Office of Management and Budget, and to report periodically to the president.

Those performance metrics are already being requested: Employees at multiple federal agencies on Saturday reported receiving an email from the **Office of Personnel Management** ordering them to reply with a set of bullet points justifying their work for the past week.

“Please reply to this email with approx. 5 bullets of what you accomplished last week and cc your manager,” the notice read. “Please do not send any classified information, links, or attachments. Deadline is this Monday at 11:59 p.m. EST.”



An email sent by the OPM to more than two million federal employees late in the afternoon EST on Saturday, Feb. 22.

In a social media post Saturday, Musk said the directive came at the behest of President Trump, and that failure to respond would be taken as a resignation. Meanwhile, Bloomberg **writes** the **Department of Justice** has been urging employees to hold off replying out of concern doing so

could trigger ethics violations. The **National Treasury Employees Union** also is **advising its employees not to respond**.

A legal battle over Trump's latest executive order is bound to join **more than 70 other lawsuits** currently underway to halt the administration's efforts to massively reduce the size of the federal workforce through layoffs, firings and attrition.

KING TRUMP?

On Feb. 15, the president posted on social media, "He who saves his Country does not violate any Law," citing a quote often attributed to the French dictator Napoleon Bonaparte. Four days later, Trump referred to himself as "the king" on social media, while the White House nonchalantly posted an illustration of him wearing a crown.

Trump has been **publicly musing about running for an unconstitutional third-term in office**, a statement that some of his supporters dismiss as Trump just trying to rile his liberal critics. However, just days after Trump began his second term, **Rep. Andy Ogles** (R-Tenn.) **introduced a bill** to amend the Constitution so that Trump — and any other future president — can be elected to serve a third term.

This week at the **Conservative Political Action Conference** (CPAC), Rep. Ogles reportedly led a group of Trump supporters calling itself the "Third Term Project," which is trying to gain support for the bill from GOP lawmakers. The event featured images of Trump depicted as Caesar.



A banner at the CPAC conference this week in support of The Third Term Project, a group of conservatives trying to gain support for a bill to amend the Constitution and allow Trump to run for a third term.

Russia continues to be among the world's top exporters of cybercrime, narcotics, money laundering, human trafficking, disinformation, war and death, and yet the Trump administration has suddenly broken with the Western world in normalizing relations with Moscow.

This week President Trump stunned U.S. allies by repeating Kremlin talking points that Ukraine is somehow responsible for Russia's invasion, and that **Ukrainian President Volodymyr Zelensky** is a "dictator." The president repeated these lies even as his administration is demanding that