

Congress of the United States

Washington, DC 20515

August 14, 2025

Donald J. Trump
President of the United States
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

Dear President Trump,

On the eve of your meeting with the murderous Russian dictator Vladimir Putin, we write to express urgent concern that your Administration is failing to address the most pressing national security threats facing our nation from Russia and our other adversaries. In the last five years, our country has endured repeated and escalating Russian attacks on US systems and infrastructure:

- The Colonial Pipeline ransomware attack (2021) by Russian criminal hackers disrupted fuel supplies across the East Coast.¹
- The JBS cyberattack (2021), also traced to Russian actors, disrupted the US meat supply chain.²

The most recent breach of the federal judiciary's electronic case filing system (CM/ECF) is a stark example of the danger. Russian-linked hackers are believed to have stolen sealed case data, source code, and information that could jeopardize witness safety and ongoing prosecutions. This is not the first such incident; an almost identical intrusion occurred in 2020 and exploited the same vulnerabilities that have gone unaddressed for five years despite repeated warnings. Today, some federal courts have been forced to revert to pen-and-paper operations to protect their most sensitive work.³

There have similarly been numerous attacks from China.

- The Chinese surveillance balloon incident (2023) traversed the continental United States collecting intelligence before being shot down.⁴
- The Chinese Communist Party state-backed hack of US government emails (2023) compromised sensitive diplomatic and security communications.⁵

¹ FBI Cyber Division briefing on Colonial Pipeline incident (May 2021). <https://www.fbi.gov/news/press-releases/fbi-deputy-director-paul-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline>

² Reuters, "JBS meat plants reopen as White House blames Russia-linked group over hack" (Jun. 2, 2021). <https://www.reuters.com/world/us/russia-linked-hacking-group-is-behind-cyberattack-against-jbs-bloomberg-news-2021-06-02/>

³ POLITICO, "A sweeping hack of the federal judiciary's case filing system..." (Aug. 2025). <https://www.politico.com/news/2025/08/12/federal-courts-hack-security-flaw-00506392>

⁴ DoD, "F-22 Safely Shoots Down Chinese Spy Balloon Off South Carolina Coast" (Feb. 4, 2023). <https://www.defense.gov/News/News-Stories/Article/article/3288543/f-22-safely-shoots-down-chinese-spy-balloon-off-south-carolina-coast/>

⁵ Reuters, "Chinese hackers stole emails from US State Dept in Microsoft breach, Senate staffer says" (Sep. 27, 2023). <https://www.reuters.com/world/us/chinese-hackers-stole-60000-emails-us-state-department-microsoft-hack-senate-2023-09-27/>

- The Volt Typhoon campaign (2023–2024) saw Chinese cyber operators target US water utilities, ports, and energy systems to pre-position for possible disruption.⁶

All of these incidents required stronger, more coordinated, and well-resourced defenses. Instead, we have seen those defenses weakened by budget cuts, workforce reductions, and the diversion of critical agencies toward low-priority political operations.

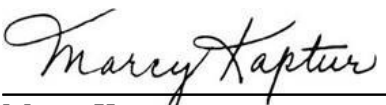
This is occurring against a backdrop of budget cuts and staffing reductions at the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA).⁷ These are the very agencies responsible for defending against such attacks, yet they have been left with fewer resources and diminished capacity. Rather than reinforcing these institutions, the Administration has repeatedly redirected their personnel to operations that offer political optics but deliver little in the way of genuine security gains.

To protect the American people and the integrity of our justice system, we respectfully urge you to:

- Address the Judiciary breach, and the broader pattern of hostile cyber activity, directly with Dictator Vladimir Putin during your upcoming meeting. You must make it clear that continued attacks will result in serious diplomatic and economic consequences.
- Fully restore and expand staffing and operational funding for DOJ, FBI, and CISA to meet the scale of today's cyber and counterintelligence threats.
- Direct a coordinated, whole-of-government initiative to close known vulnerabilities in the judiciary's CM/ECF system and other high-risk federal networks.

The safety of our citizens, the resilience of our critical systems, and the credibility of our national security posture depend on confronting real threats with urgency and resolve, rather than diverting attention to operations that serve political ends while leaving our defenses exposed. We can and we must do better to face the pressing national security threats we face from cyberattacks. We urge you to please act on these matters with haste and resolve.

Sincerely,



Marcy Kaptur
Member of Congress



Julie Johnson
Member of Congress

⁶ CISA, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure" (Feb. 7, 2024) <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>

⁷ Congressional Research Service reports on DOJ, FBI, and CISA staffing levels, FY2025 appropriations. <https://www.congress.gov/crs-product/R48189>

A handwritten signature in black ink, appearing to read 'Dan Goldman', written over a horizontal line.

Dan Goldman
Member of Congress

A handwritten signature in blue ink, appearing to read 'Lloyd Doggett', written over a horizontal line.

Lloyd Doggett
Member of Congress

CC: Attorney General Pam Bondi, FBI Director Kash Patel, and CISA Director Madhu
Gottumukkala