

NetChoice

September 9, 2024

The Honorable Robin Carnahan
Administrator
General Services Administration
1800 F Street NW
Washington DC 20405

Dear Administrator Carnahan:

We write to express significant concerns with the July 2024 global IT outage involving Microsoft and CrowdStrike. The widespread nature of the outage and its profound impact underscores the urgent need to address the implications of single points of failure in America's critical IT infrastructure.

NetChoice is a trade association of leading e-commerce and online companies promoting the value, convenience, and choice of internet business models. Our mission is to make the internet safe for free enterprise and for free expression. We work to promote the integrity and availability of the global internet and are significantly engaged in issues in the states, in Washington, and in international internet governance organizations.

On July 19, a routine update to CrowdStrike's Falcon Sensor software inadvertently caused widespread disruptions for Microsoft Windows users globally. This update led to critical system failures, including so-called "Blue Screen of Death" errors and boot loops, affecting approximately 8.5 million devices worldwide. The outages disrupted a wide range of sectors including airlines, emergency room services, financial institutions, and the federal government.

The outage made clear that Microsoft software sits at the foundation of many critical industries. According to one estimate, this outage cost businesses \$5.4 billion¹ - yet only affected 1%² of Microsoft's systems globally.

1

<https://www.reuters.com/technology/fortune-500-firms-see-54-bln-crowdstrike-losses-says-insurer-parametrix-2024-07-24/>

² <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>

Our concerns are compounded by the fact that Microsoft is the leading provider of productivity software, cloud services and security technology to the federal government. In fact, the company has a dominant 85% market share³ in the U.S. government’s productivity software market, which we believe poses an acute national security risk and threatens the disruption of essential services millions of Americans depend on every day.

After the release of the Cyber Safety Review Board’s report on the 2023 Microsoft Online Exchange Incident, Microsoft pledged to put security “above all else” on May 3, 2024.⁴ Since then, we have tracked 65 additional security incidents and vulnerabilities. These are listed on our site tracking these incidents, [MicrosoftVulnerabilityTracker.com](https://microsoftvulnerabilitytracker.com/).⁵

Additionally, we conducted research shortly after the outage and found that it was a crystallizing moment in the public’s minds about the risk of overreliance on Microsoft. In a survey of 1,031 registered voters, 62% of respondents were more concerned after the outage about Microsoft’s market share in government and critical infrastructure software and services. The majority of survey respondents (65%) also think the U.S. government needs to change how it uses Microsoft products.⁶

Overdependence on Microsoft’s insecure software and cloud products has created single points of failure in many critical industries—we saw this with the outage, when a small percentage of Microsoft devices crippled IT systems globally. Without addressing this overdependence within the federal government, America’s critical IT infrastructure will remain vulnerable to cybersecurity threats that will continue to increase in potential scope and magnitude.

We call on you to listen to the public and address the urgent need to change how the government uses and contracts its critical IT infrastructure—and to do so before the inevitable next security incident.

Sincerely,
Amy Bos
Director of State and Federal Affairs, NetChoice

3

<https://omdia.tech.informa.com/-/media/tech/omdia/marketing/commissioned-research/pdfs/monoculture-and-market-share-the-state-of-communications-and-collaboration-software-in-the-us-government-v3.pdf?rev=8d41cc2d16de491b9f59d2906309fdaa>

⁴ <https://blogs.microsoft.com/blog/2024/05/03/prioritizing-security-above-all-else/>

⁵ <https://microsoftvulnerabilitytracker.com/>

6

<https://netchoice.org/new-poll-americans-concerned-about-government-cybersecurity-following-microsoft-crowds-trike-outage/>