United States Senate

WASHINGTON, DC 20510

September 9, 2024

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

Dear Administrator Carnahan:

We write today to express our concerns about the widespread disruptions that occurred across the federal government due to the Microsoft Windows and CrowdStrike outage. On July 19, 2024, the cybersecurity firm CrowdStrike pushed a faulty update to its users running Microsoft Windows operating systems.[1] The update crippled small businesses, companies, and government services worldwide. Agencies across the federal government experienced a range of service disruptions. For example, the Social Security Administration shuttered offices,[2] Customs and Border Protection experienced processing delays,[3] and Indian Health Service clinics experienced service disruptions.[4] The outage slowed or stopped operations across the federal government and our constituents were unable to access government services they rely on.

The General Services Administration (GSA) is responsible for negotiating procurement contracts for federal agencies. As such, your team should be able to provide insight into the incident and into possible similar vulnerabilities across the federal government's information technology (IT) systems. As demonstrated by this outage, there are risks to relying on too few contractors to operate such a large share of the federal government's IT systems; this is particularly true for software that has kernel access and high-level privileges to critical government systems. Your agency should ensure that the IT systems our country relies on are as secure and resilient as possible. This includes considering any potential reliability and security threats that could be mitigated through increased supply chain diversification.

To better understand the extent of the CrowdStrike incident's impacts on the federal government and any similar vulnerabilities, please provide answers to the following questions by September 30, 2024.

[1] Sam Schechner, Gareth Vipers, Alyssa Lukpat, *Major Tech Outage Grounds Flights, Hits Banks and Businesses Worldwide*, THE WALL STREET JOURNAL (July 19, 2024), *available at* https://www.wsj.com/tech/microsoft-reports-major-service-outage-affecting-users-worldwide-328a2f40.

[2] John Cohen, "Federal Government Agencies Affected by Worldwide IT Outage," FedScoop, July 28, 2023, https://fedscoop.com/federal-government-agencies-affected-by-worldwide-it-outage/.

[3] Rachel Lerman, "How a CrowdStrike Cybersecurity Fix Caused a Global Mess for Microsoft," *The Seattle Times*, July 29, 2023, https://www.seattletimes.com/business/technology/how-a-crowdstrike-cybersecurity-fix-caused-a-global-mess-for-microsoft/.

[4] "Renata Birkenbuel," "Global Tech Outage Affects Some Indian Health Clinics," *ICT News*, July 31, 2023, https://ictnews.org/news/global-tech-outage-affects-some-indian-health-clinics-.

1. Is GSA able to provide a full list of federal agencies that utilize CrowdStrike products? If not, why is GSA unable to do so? Which entity would be able to provide this information?

2. Is GSA able to provide the most current list of federal agencies that were impacted by the outages caused by the faulty CrowdStrike update? If not, why is GSA unable to do so? Which entity would be able to provide this information?

3. Are there any software procurement contract requirements that should have mitigated this outage? If not, what steps will GSA take to update procurement contracts to ensure software has the appropriate deployment, maintenance, and testing plans in place?

4. What steps has GSA taken to engage with CrowdStrike since the outage? How is GSA working with CrowdStrike to prevent future incidents?

5. What other software used by Federal agencies have the same level of privilege, namely kernel access? Is GSA able to provide a list of the service type, provider, and the utilizing agencies? If not, why is GSA unable to do so? Which entity would be able to provide this information?

6. Does GSA have a risk assessment and evaluation process in place to understand and account for the risk posed by software with kernel access? Does GSA consider risks of overreliance—of both the software service and the underlying operating systems they run on—when making procurement choices available to federal agencies?
    a. If so, please provide a copy of any relevant guidance or policies.
    b. If not, how does your agency plan to account for these risks moving forward?

7. Does GSA currently consider, including consultation with the proper agencies, the national security implications of overreliance on one contractor when making procurement decisions? If not, will your agency commit to doing so moving forward?

Thank you for your attention to this important matter.

Sincerely,

Brian Schatz
Brian Schatz
United States Senator

Peter Welch
Peter Welch
United States Senator