One social factor leading to the publishing of Executive Order 14028, Improving the Nation's Cybersecurity, is Americans' dependence on tech and the growing fears of said tech being compromised. There is an emphasis in the EO 14208 to regulate the private sector, and this comes as no surprise when Americans' "feelings about private industry, roughly six-in-ten Americans feel that U.S. businesses themselves are very (9%) or somewhat (52%) prepared to prevent cyberattacks on their own systems" (Olmstead & Smith, 2022). Additionally, "when it comes to the U.S. government's preparedness to handle these attacks, around six-in-ten Americans feel that the government is very (13%) or somewhat (49%) prepared to prevent a cyberattack on our public infrastructure" (Olmstead & Smith, 2022). The glass-is-half-full perspective is turning, and soon, Americans may see the glass as half-empty when it comes to the federal government's ability to protect its private citizens in Cyberspace. Especially in the world of federal contractors, as this group is marginally impacted by the requirements President Bident outlined in EO 14208. The U.S. General Services Administration emphasizes "modification of contract language to reflect new guidance from NIST and CISA. If your company cannot accept the modification, you cannot sell to the Federal government" (*Executive Order 14028: Improving the Nation's Cybersecurity*, n.d.). Private contractors are forced to uphold our face bankruptcy, a social consequence most companies rather avoid. On the flip side, companies like Archon help by acting as a solution in response to EO 14098, such as "next-gen, end-user devices to [their] hardware and data services, Archon Secure provides CSfC solutions that are customizable, scalable, and NSA-compliant" (ID Technologies, 2022). Private contractors have help if they need it to become up to standards, as in "the time periods within which contractors must report cyber incidents based on a graduated scale of severity, with reporting on the most severe cyber incidents not to exceed three days after initial detection" in the Cyberworld if they are to

continue doing business with the United States federal government (Biden, 2022). To put it another way, on one end, private contractors are arguably being put out, especially when smaller private government contracting companies may not have the infrastructure to support such strict timelines, but companies like Archon Secure may be able to help these contracting companies.

To reflect on the above and review how the subcultural of the Democratic party has shaped President Biden's EO 14208. From threats of election fraud to "the largest-ever investment in the nation's cybersecurity is hanging in the balance as Democrats continue to spar over two mammoth spending bills" (Marks, 2021). Solutions are not a size fit all when it comes to America's Cybersecurity, but all of the solutions cost money, a lot of money, and Marks notes intelligence officials have treated cyberthreats with responses equivalent to terrorism "[but] Washington has never invested in protecting the nation's critical infrastructure against cyberattacks in the way it surged funding to terrorism protections after 9/1" (2022). Therefore, President Biden's EO 14208 is the push Washington needed to direct funding to an area that has long been underfundedunderfunded. The influence to note here is the lack of money in one area urging a political discussion loud enough to enforce an executive order. Especially when there is such a reliance on tech from both the public and private sectors within the United States and growing fears of these devices and systems being compromised. Trust is a fickle thing, changing from year to year. This is no truer than for the general public opinion in the federal government and members on the Hill. As such, it can be a reasonable assumption that the Democrat's and Republican's short sidedness in the past towards Cybersecurity budgeting, the public's increased use of devices and systems connected in Cyberspace, and the increased reliance on private government contracting to achieve secure Cyberspace, led to the President Biden's Executive Order to improve the nation's cybersecurity.

References

Biden Jr., J. R. (2021). Executive Order 14028--Improving the Nation's Cybersecurity. *Daily Compilation of Presidential Documents*, 1–15. Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Executive Order 14028: Improving the Nation's Cybersecurity. (n.d.). Retrieved From https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity.

ID Technologies. (2022, April 28). *Archon Secure responds to Executive Order 14028* [Video]. YouTube. Retrieved From https://www.youtube.com/watch?v=6R0_tKYfejQ.

Marks, J. (2021, November 2). *Cybersecurity funding is at stake in Democrats' spending battles*. Washington Post. Retrieved From https://www.washingtonpost.com/politics/2021/11/02/cybersecurity-funding-is-stake-democrats-spending-battles/.

Olmstead, K., & Smith, A. (2022, September 15). *Americans and Cybersecurity*. Pew Research Center: Internet, Science & Tech. Retrieved From https://www.pewresearch.org/internet/2017/01/26/3-attitudes-about-cybersecurity-policy/.