The cost for the general public is increased data collection concerning such groups' rights. However, there is still speculation whether or not this is being appropriately handled, but President Biden, in his Executive Order 14208, Improving the Nation's Cybersecurity, does address the concern. There is also growing concern within the private government contracting group on whether or not smaller entities can compete with bigger contracting groups because of the EO 14208 timeline requirements, which is not a point of concern directly addressed in the EO 14208.

The first ethical implication for the general public includes concerns about privacy and data overcollection, beginning with the readability of programs' terms and conditions to ensure efficient federal government oversight in secure cyberspace. President Biden, in his Executive Order 14208, Improving the Nation's Cybersecurity in "modernizing Federal Government Cybersecurity…increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties" (2021, p. 1). Following along in the privacy concern is contract language in the way of readability for users and consumers. There is much debate about where the ethical line is. Although most agree, permission statements, terms of conditions, privacy policies, and notification of a change in these should be understandable. Jayati Dev et al. write, "privacy policies are more opaque and less accessible. Presidential Executive Order 14028 requires a robust 'labeling program' for consumers to know how their data is being collected, used, and stored" (2021, p.3). To increase readability, Dev et al. and team introduce the "Step-by-Step Approach to Module Labels," including users' ability on a "personal interface" to "update their preferences at any time," transparency concerning the "what," "how," and "how long" of data, and the sectioning of a systems privacy policy (2021, pp. 2-3). Arguably a response prompted by the EO 14208 executive order to help curate a more ethical line concerning user privacy rights in cyberspace. The NIST also responded to EO 14208 requirements in the creating of "two labeling programs [relating[to the Internet of Things (IoT) and software to inform consumers" (*NIST Issues Guidance on Software, IoT Security and Labeling | NIST*, 2022). Considering we have entered into In an age where, as Pendino et al., writes

"the United States is under stack in the cyber domain," and inserts policymakers should change public perception and "narrative, moving away from a language of fear and toward a notion of cyber as a domain of warfare" (2022).

Another ethical implication exists within the private government contractor community in reaction to EO 14208. There is speculation that smaller contract companies cannot keep up with the 14028 Presidential Executive Order's timeline. It is prompting a discussion revolving around whether or not smaller private government contractors will be able to compete in the coming decade at the time. Especially when the Department of Defense, in a "response to President Biden's Executive Order 14017" addressing the essential role the community of smaller businesses and smaller private government contractors were "key members of DoD supply chains" (*Securing Defense-Critical Supply Chains*, 2022, p. 7). Additionally, competition "may drive contractors lowest cost" (p. 20), where more prominent private government contractors can eat costs and losses more so than smaller companies. Keeping the previous EO in mind, this brought forward the same question when the 14028 EO emphasized an even greater push for increased oversight in data privacy and securing a good supply chain. In a world where "President Biden's Executive Order directs sweeping changes to cybersecurity requirements in federal government contracts and calls for the government to 'bear the full scope of its authorities and resources'" (*Cybersecurity Executive Order Will Impact Government Contractors*, n.d.). Does increasing oversight mean increasing the numbers within an organization, and where does this leave smaller private government contractors?

EO 14028 puts the American government's best foot forward in discussing an individual's data rights. However, there is much to see for future cybersecurity policies within the federal government. Also, smaller private government contractors must grapple with increasing budgets or suffer potential revenue losses. Both ethical implications leave many questions on the table, is there room for data privacy rights in a cyber war, and what type of companies can sit at the table?

References

Biden Jr., J. R. (2021). Executive Order 14028--Improving the Nation's Cybersecurity. *Daily Compilation of Presidential Documents*, 1–15. Retrieved from http://proxy.lib.odu.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=150508114&scope=site.

Cybersecurity Executive Order Will Impact Government Contractors. (n.d.). Pillsbury Law. Retrieved From https://www.pillsburylaw.com/en/news-and-insights/cybersecurity-executive-order-government-contractors.html.

Dev, J., Gopavaram, S., Gumusel, E., & Camp, J. (2021). *A Consumer-focused Modular Approach to Labeling IoT Devices and Software*. Retrieved From nist.gov. https://www.nist.gov/system/files/documents/2021/11/04/IndianaUniversity-NIST_Modular_Labels.pdf.

NIST Issues Guidance on Software, IoT Security and Labeling | NIST. (2022, February 4). NIST. Retrieved From https://www.nist.gov/news-events/news/2022/02/nist-issues-guidance-software-iot-security-and-labeling.

Pendino, S., Jahn, R., & Pedersen, K. (2022). U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light. *ACADEMIC JOURNALS*. Retrieved From https://jfsc.ndu.edu/Media/Campaigning-Journals/Academic-Journals-View/Article/3149856/us-cyber-deterrence-bringing-offensive-capabilities-into-the-light/.

Securing Defense-Critical Supply Chains. (2022, February). defense.gov. Retrieved From https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF.