Social Implications of Executive Order 14028

Elijah Gartrell

Old Dominion University

CYSE 425W

Professor Bora Aslan

11/24/2024

Social Implications of EO 14028

Executive Order (EO) 14028, signed in May 2021, represents a significant step in addressing cybersecurity challenges in the United States. While designed to enhance the security of government and private networks, it also carries important social implications, such as its effects on privacy, equity, and public-private collaboration. This policy reflects how cybersecurity measures intersect with societal values and responsibilities in an increasingly digital world.

The implementation of EO 14028 encourages greater accountability and vigilance in cybersecurity practices. By requiring federal agencies and contractors to adopt zero-trust architecture and stricter supply chain protections, the policy pushes for broader adherence to secure online behaviors. These measures aim to safeguard personal and national security but raise concerns about the trade-off between security and privacy. For example, increased government data-sharing and logging practices can lead to fears of over-surveillance. Such apprehension might discourage free expression and erode trust in digital spaces. Balancing security needs with privacy protections is crucial to addressing these societal concerns.

EO 14028 also highlights issues of equity within digital spaces. Marginalized communities often lack access to resources or education needed to navigate cybersecurity challenges, leaving them more vulnerable to exploitation. Without targeted initiatives to address these disparities, the order risks widening the digital divide. Policymakers must ensure equitable access to cybersecurity tools and education to help close these gaps and extend the benefits of improved security to all demographics.

Cultural and societal attitudes toward privacy have also shaped the development of EO 14028. In the United States, the value placed on individual freedoms has often fueled resistance to policies perceived as invasive. Policymakers have responded by emphasizing transparency and accountability in implementing this order. However, achieving a balance between protecting individual rights and implementing effective cybersecurity measures remains an ongoing challenge. The policy reflects the tension between privacy advocates, who call for stricter limits on government oversight, and those who prioritize robust security measures for critical infrastructure. Businesses, particularly those working with the government, face significant pressure under EO 14028. While larger companies often have the resources to meet stricter cybersecurity standards, smaller businesses may struggle to comply. These disparities raise concerns about fairness in the business landscape, with some entities potentially being excluded from lucrative opportunities due to resource limitations. Nevertheless, the emphasis on public-private collaboration illustrates the importance of shared responsibility in combating cyber threats.

EO 14028 demonstrates how cybersecurity policies can influence society beyond their technical goals. By encouraging secure practices while addressing privacy concerns and equity issues, the order highlights the need for a careful balance between protection and fairness. As the policy evolves, its ability to foster trust and inclusivity will determine its long-term impact on the digital and social fabric of the nation. EO 14028 is more than just a government plan for stronger cybersecurity. It’s a reflection of how society views privacy, fairness, and responsibility. While the order is designed to make the country safer, it also brings challenges, like figuring out how to protect privacy and ensuring that everyone benefits equally from these changes. The decisions

made now will not only shape how secure systems are but also how people trust and interact with the government and technology in the future.

References

U.S. Government Accountability Office. (2021). Federal cybersecurity: Federal agencies need to implement foundational cyber hygiene practices. U.S. Government Accountability Office. https://www.gao.gov/assets/d24106343.pdf

DirectDefense, Inc. (2021). Strengthening national cybersecurity: Executive Order 14028 and its implications. DirectDefense. https://www.dirsec.com/insights/strengthening-national-cybersecurity-executive-order-14028-and-its-implications/

BizTechReports. (2022, January 13). Impact of Executive Order 14028 on developing secure architectures across multi-cloud infrastructures. BizTechReports. https://www.biztechreports.com/news-archive/2022/1/13/impact-of-executive-order-14028-on-developing-secure-architectures-across-multi-cloud-infrastructures

DeGast, A. (2021, August 13). Federal cybersecurity update: Executive Order 14028 implications for agencies and vendors. Security Intelligence. https://securityintelligence.com/news/executive-order-14028-federal-cybersecurity-update/