Biden’s Executive Orders on Digital Activity
Victoria Cerrone, Chief Growth Officer, Resiliant

President Biden’s executive order, issued on October 30, 2023, emphasizes the importance of managing the risks associated with artificial intelligence (AI), especially concerning safety, security, and privacy. The Biden administration is now preparing another executive order to safeguard US personal data from foreign adversaries, which is expected to restrict highly sensitive data, such as genetic and location information, from foreign entities' access through legal mechanisms. It targets data transactions that could provide adversarial countries with sensitive personal or government-related data, highlighting concerns over using artificial intelligence for data mining and profiling by foreign nations. The aim is to create a comprehensive US data privacy and security standard, addressing this area's absence of federal legislation.

Why did this occur?

An exponential increase in digital activity following the COVID-19 pandemic has resulted in an uncontrolled and broad global exposure of personally sensitive data that consumers and businesses alike did not bargain for. Consumers are used to friction-free web access and have a basic expectation of privacy protection from the companies they deal with. Those companies say they protect the user's private information - that is - until it's hacked or sold to third parties without user permission or knowledge. Companies also take advantage of collecting and storing personal data under the guise of providing better and more personalized services and products. However, no business is exempt from data privacy compliance.

The impact of these initiatives on small businesses could be significant. For one, small businesses may need to adapt to tighter regulations and standards concerning data privacy and AI. They must ensure their practices comply with the new federal guidelines, which could involve updating their data management and cybersecurity measures. While this may initially pose challenges, particularly for those with limited resources, it also allows small businesses to build trust with their customers by demonstrating a commitment to protecting sensitive information and ethical AI use.

On another note, the push towards privacy-preserving technologies and the emphasis on AI safety and security could spur innovation in the small business sector. Companies that can adapt and offer secure, privacy-focused services and products may find new market opportunities, especially as consumers become more aware of data privacy and security issues.

With the new orders, small businesses face more complex data protection and privacy regulations without knowing how to effectively change their aging legacy systems and networks on a limited budget. They need a low-cost, proactive, and efficient Zero Trust security model that removes the burden of handling and storing unnecessary consumer data. The key is user empowerment - restoring the user's control over their data. This allows users to make informed choices about their privacy settings and data-sharing preferences. For small enterprise, giving

customers control over their personal data is the best way to reduce risk, build trust, enhance reputation, secure competitive advantage, and comply with all data and privacy protection regulations.

RESILIANT next-generation digital identity and Identity-First cybersecurity solutions put the user in control of their data. We employ blockchain and AI technology to ensure that sensitive user data remains unexposed and is not stored in the cloud. This allows for the seamless transfer of information without compromising user credentials. All RESILIANT solutions automatically comply with privacy regulations, data management standards (GDPR, ISO), and zero trust architecture models (NIST, CISA, EO 14028) by nature of the system and its features.

For more information, please visit: https://www.carahsoft.com/resiliant

RESILIANT

carahsoft.

Biden's Executive Orders on Digital Activity
Victoria Cerrone, Chief Growth Officer, Resiliant

President Biden's executive order, issued on October 30, 2023, emphasizes the importance of managing the risks associated with artificial intelligence (AI), especially concerning safety, security, and privacy. The Biden administration is now preparing another executive order to safeguard US personal data from foreign adversaries, which is expected to restrict highly sensitive data, such as genetic and location information, from foreign entities' access through legal mechanisms. It targets data transactions that could provide adversarial countries with sensitive personal or government-related data, highlighting concerns over using artificial intelligence for data mining and profiling by foreign nations. The aim is to create a comprehensive US data privacy and security standard, addressing this area's absence of federal legislation.

Why did this occur?

An exponential increase in digital activity following the COVID-19 pandemic has resulted in an uncontrolled and broad global exposure of personally sensitive data that consumers and businesses alike did not bargain for. Consumers are used to friction-free web access and have a basic expectation of privacy protection from the companies they deal with. Those companies say they protect the user's private information - that is – until it's hacked or sold to third parties without user permission or knowledge. Companies also take advantage of collecting and storing personal data under the guise of providing better and more personalized services and products. However, no business is exempt from data privacy compliance.

The impact of these initiatives on small businesses could be significant. For one, small businesses may need to adapt to tighter regulations and standards concerning data privacy and AI. They must ensure their practices comply with the new federal guidelines, which could involve updating their data management and cybersecurity measures. While this may initially pose challenges, particularly for those with limited resources, it also allows small businesses to build trust with their customers by demonstrating a commitment to protecting sensitive information and ethical AI use.

On another note, the push towards privacy-preserving technologies and the emphasis on AI safety and security could spur innovation in the small business sector. Companies that can adapt and offer secure, privacy-focused services and products may find new market opportunities, especially as consumers become more aware of data privacy and security issues.

With the new orders, small businesses face more complex data protection and privacy regulations without knowing how to effectively change their aging legacy systems and networks on a limited budget. They need a low-cost, proactive, and efficient Zero Trust security model that removes the burden of handling and storing unnecessary consumer data. The key is user empowerment - restoring the user's control over their data. This allows users to make informed choices about their privacy settings and data-sharing preferences. For small enterprise, giving

Biden's Executive Orders on Digital Activity

By: Victoria Cerrone, Chief Growth Officer, Resiliant

Thank you for downloading this Resiliant resource. Carahsoft is the Master Government Aggregator for Resiliant solutions available via NASA SEWP V, ITES-SW2, NASPO ValuePoint and other contract vehicles.

To learn how to take the next step toward acquiring Resiliant's solutions, please check out the following resources and information:

For additional resources:
www.carahsoft.com/resiliant/resources

For upcoming events:
www.carahsoft.com/resiliant

For additional Resiliant solutions:
www.carahsoft.com/resiliant/solutions

For additional Cyber solutions:
carah.io/cybersolutions

To set up a meeting:
resiliant@carahsoft.com
(703) 871-8548

To purchase, check out the contract vehicles available for procurement:
www.carahsoft.com/resiliant/contracts