IOWA
Public Policy Center

POLICY BRIEF
November 2022

# ENHANCING CYBERSECURITY TO PROTECT AMERICA'S DATA

**Samuel Rich**
Undergraduate Student, Department of Political Science

Between 2010 and 2020, more than 38 billion records were exposed by 40,000 data hacks. Although many of these hacks were carried out on a smaller, less harmful scale, several gained access to government records and the records of millions of Americans. Large-scale data breaches have been occurring at an increasing rate, especially due to the support these hacking groups receive from countries such as Russia, China, Iran, and North Korea.[1] These attacks have demonstrated a need to update U.S. cybersecurity measures to protect against further intrusions. While there are new and emerging methods to strengthen cybersecurity, the Cybersecurity and Infrastructure Security Agency (CISA) and other federal agencies conducting information technology (IT) research should begin to research and develop a sustainable blockchain model to protect sensitive government data against cyberattacks.

## The Federal Government's Vulnerability to Cyberattacks

In May 2021, President Biden signed the "Executive Order on Improving the Nation's Cybersecurity," which outlined policies intended to prevent, detect, assess, and remediate future cyber incidents.[2] This executive order was in response to several cyberattacks that federal agencies have experienced in recent years and showcased the Biden Administration's commitment to protecting federal agencies from future cyberattacks. In 2015, the U.S. Office of Personnel and Management (OPM) discovered two separate, but related, cyber breaches. With the discovery of the first breach in early 2015, OPM found that 4.2 million current and former employees of the federal government had their personal data stolen. Then, in June of the same year, OPM discovered that the background investigation records of 21.5 million individuals had been breached. These records included information such as the Social Security numbers of current, former, and potential federal employees and contractors.[3]

In November 2020, a cybersecurity firm reported a breach in a cyber platform established by the network management software company SolarWinds. The breach was initiated by the Russian Foreign Intelligence Service (SVR) in February 2019 by placing malware in an update to SolarWinds' network management and monitoring products. By hacking into this network, the Russian SVR was granted unauthorized access to the data of an estimated 18,000 SolarWinds customers, including the unclassified systems of several federal agencies.[4] Some of the most consequential breaches included the intrusion into the Treasury Department's email system, as well as software at the Los Alamos National Laboratory, which develops and designs nuclear weapons. The SVR was also able to access several technology and service providers of the government, including Microsoft, Cisco, and CrowdStrike, despite some not employing SolarWinds technology.[5]

These cyberattacks prompted Congress to greatly increase the federal IT budget. It is estimated that the budget for IT at federal agencies in FY 2023 will be $65 billion, with $10.9 billion for civilian cybersecurity. The large budget allows for the delivery of critical citizen services and protection of sensitive data and systems, and it enables planning, oversight, funding, accountability, and guidance across federal agencies.[6] CISA also received a $334 million increase in funding after the House Appropriations Homeland Security Subcommittee approved a $2.93 billion budget.[7]

## Blockchain Could Improve Cybersecurity and Reduce Costs

In the past decade, there has been a sharp increase in the use of blockchain technology throughout several industries, with the most well-known application being in the development of cryptocurrencies like Bitcoin. Blockchain enables a quick, trustworthy, and verifiable transfer of data from one party to another without the need for certification by a third party. Blockchain's most innovative characteristics are high service availability and data integrity. High service availability allows a network to continue operating even if a critical component fails, while data integrity verifies the trustworthiness of incoming and outgoing data. Due to blockchain's unique characteristics, it has evolved from a technology that enables the transfer of cyptocurrencies to a secure data storage method that is being implemented in several industries and governments.[8] Blockchain has also gained popularity due to its use of Distributed-Ledger Technology (DLT), which provides a decentralized technological network to securely exchange internet-based data between information systems.[7]

While not on a large scale, blockchain has been introduced to the U.S. Government through the Department of Health and Human Services' (HHS) *Accelerate* program. *Accelerate* is used to manage 100,000 HHS contracts totaling around $25 billion and is estimated to have saved HHS $720 million at the point of purchase. The blockchain utilized in *Accelerate* uses an indicator of unstructured data instead of saving the actual data, which adds an extra layer of security to the storage of personal information.[9] *Accelerate* has been instrumental in cutting costs and securing data for HHS, but there is little consensus about the implementation of blockchain throughout government agencies. For blockchain to prove effective in government, skeptics believe there needs to be a focus on building right use cases and establishing a scalable deployment approach.

## Policy Recommendation

Due to the increasing number of cyberattacks, it is essential that federal agencies implement new cybersecurity methods to detect and defend against attacks on stored data. While blockchain is a new technology, it has proven to be a secure storage method that can reduce contract fees for federal agencies by eliminating the need for certification by a third party. Some cybersecurity experts remain skeptical of blockchain's implementation throughout federal agencies. Due to the concerns of these experts, this policy brief does not advocate for the immediate implementation of blockchain throughout all federal agencies. Blockchain has proved to be effective in the case of Health and Human Services, but the skeptics could be right about blockchain only being effective in some cases throughout the government. Instead of focusing on the immediate implementation of blockchain, CISA and other federal agencies conducting IT research should focus their research on the development of a sustainable blockchain model capable of protecting and defending against future cyberattacks.

# References


[1] Leonhardt, Megan. "The 10 Biggest Data Hacks of the Decade." CNBC. CNBC, December 27, 2019. https://www.cnbc.com/2019/12/23/the-10-biggest-data-hacks-of-the-decade.html

[2] Biden, Joseph. "Executive Order on Improving the Nation's Cybersecurity." The White House. The United States Government, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[3] "Cybersecurity Resource Center Cybersecurity Incidents." U.S. Office of Personnel Management. Accessed September 30, 2022. https://www.opm.gov/cybersecurity/cybersecurity-incidents/

[4] Office, U.S. Government Accountability. "Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents." Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents | U.S. GAO, February 8, 2022. https://www.gao.gov/products/gao-22-104746

[5] Wolff, E. D., Growley, K. M., Lerner, M. O., Welling, M. B., Gruden, M.G., & Canter, J. (2021). Navigating the SolarWinds Supply Chain Attack. *Procurement Lawyer, 56(2), Pg. 3-4* https://www.crowell.com/files/20210325-Navigating-the-SolarWinds-Supply-Chain-Attack%20.pdf

[6] "16. Information Technology and Cybersecurity Funding – White House." The White House, 2022 https://www.whitehouse.gov/wp-content/uploads/2022/03/ap_16_it_fy2023.**pdf**

[7] Kagubare, Ines. "House Subcommittee Approves $334 Million Funding Bump for Cisa." The Hill. The Hill, June 16, 2022. https://thehill.com/policy/cybersecurity/3526827-house-subcommittee-approves-334-million-funding-bump-for-cisa/

[8] Clavin, James, Duan, Sisi, Zhang, Haibin, et al. "Blockchains for Government: Use Cases and Challenges: Digital Government: Research and Practice: Vol 1, No 3." Digital Government: Research and Practie, July 1, 2020. https://dl.acm.org/doi/10.1145/3427097

[9] Pandey, Ameep. "How Governments Can Harness the Potential of Blockchain." McKinsey & Company, November 6, 2020. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/how-governments-can-harness-the-potential-of-blockchain.