

AGENCIES IMPLEMENT TECHNOLOGY Executive Orders

INSIDE:

- The White House's
AI Executive Order 3
- Infographic:
Cybersecurity Goals 7
- Orders' Impact on
Tech Modernization 9
- Improving Digital
Customer Experience ... 13
- Sidebar:
AI Chiefs at Agencies. ... 16

SPONSORED BY



U.S. Government Solutions

From the editor's desk



Ross Gianfortune, Managing Editor

Executive Action For Tech Leadership

Establishing the United States as a global technology leader has been a goal of every presidential administration for decades. Since coming into office, President Joe Biden's administration has followed this trend by signing a series of tech-related executive orders. In 2021, the White House's order on Improving the Nation's Cybersecurity established goals and requirements for agencies to implement and face the cyber challenge.

Digital government customer service is the subject of a 2021 order that requires agencies integrate human-centered design and digital service concepts. Streamlining access to agencies is among the goals of the order, with agencies using digital services

to reduce friction between the public and government.

Artificial intelligence is the latest frontier that the White House hopes to lead. The October AI executive order seeks to create baselines for the technology, guidance for ethical AI and reinforce the United States as an AI research and implementation leader. The lengthy order also calls for agencies to establish chief artificial intelligence officers to lead their agencies' pursuit of promoting innovation and managing AI risks.

When introducing the AI order and discussing priorities to advance America's leadership in technology, Biden said, "I'm determined to do everything in my power to promote and demand responsible innovation." ❁

Table of Contents



Ross Gianfortune,
Managing Editor



Jordan McDonald
Staff Writer



ARTICLE

White House Aims to Cut AI Risks to National Security with New Regulations

The order tasks agencies with creating standards for secure AI and developing 'game-changing cyber protections.'



INFOGRAPHIC

Key Goals of the Cybersecurity Executive Order

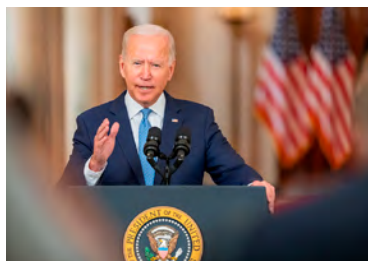
As cyber threats evolve, agencies need to prevent, disrupt and mitigate attacks. Signed in 2021, the White House Executive Order on Improving the Nation's Cybersecurity outlined a more comprehensive approach to securing networks, requiring agencies to shift toward stronger cyber standards and to adopt advanced security solutions.



PARTNER INTERVIEW

Executive Orders' Impact on Tech Modernization

Jose Padin, Chief Transformation Officer, U.S. Public Sector, Zscaler



ARTICLE

Customer Experience Tech Improvements Highlight Biden Executive Order

Agencies are integrating human-centered design principles to improve customer-facing digital platforms and align with the executive order.



ARTICLE

The CAIOs Leading Responsible AI Development Across Government

Since the White House's AI executive order was released, federal agencies are in the process of naming chief artificial intelligence officers.

White House Aims to Cut AI Risks to National Security with New Regulations

The order tasks agencies with creating standards for secure AI and developing ‘game-changing cyber protections.’

The White House’s artificial intelligence executive order seeks to manage risks that the nascent technology poses to national security, IT systems and economic security.

The executive order is being touted by the Biden-Harris administration as “the most sweeping actions ever taken to protect Americans from the potential risks of AI systems.” It directs federal agencies to develop standards for secure AI and address the risks that the emerging technology may pose to chemical, biological, radiological, nuclear and cybersecurity systems.

“This order builds on the critical steps we’ve already taken,” President Joe Biden said at an event introducing the order. “With today’s executive order I’ll soon be signing, I’m determined to do everything in my power to promote and demand responsible innovation.”

Through the Defense Production Act, companies developing large-scale AI systems potentially posing national security risks are now required to share their safety test results with the federal government.

The executive order also directs the Defense Department and the Department of Homeland Security to complete an operational pilot project



that will deploy AI capabilities, including large language models to help find and remediate vulnerabilities in the federal government’s software, systems and networks.

“In the wrong hands, AI can make it easier for hackers to exploit vulnerabilities in the software that makes our society run. That’s why I’m directing



the Department of Defense and Department of Homeland Security, both of them, to develop game-changing cyber protections that will make our computers and our critical infrastructure more secure than it is today,” Biden said.

Requirements for the Defense Department

The executive order directs the secretary of defense to assess ways AI can increase biosecurity risks and make recommendations on how to mitigate those risks. Risks from generative AI models trained on biological data are of particular concern.

Another section of the executive order said the secretary of defense, alongside the director of national intelligence and secretaries of energy, commerce and homeland security, will develop initial guidelines for performing security reviews. These guidelines will include reviews that identify risks posed by the release of federal data that could help develop offensive cyber capabilities or chemical, biological, radiological and nuclear weapons.

The order also directs DOD to address gaps in AI talent. It requires the DOD to make recommendations on how to hire noncitizens with certain skill sets, including at the Science and Technology Reinvention Laboratories. The secretary of defense will also make recommendations to streamline processes for accessing certain classified information for noncitizens.

The executive order outlines a critical role for DHS in mitigating AI’s risks to critical infrastructure. It calls for the agency to develop secure standards, tools and tests for AI deployment.

“[The President’s Executive Order] directs DHS to manage AI in critical infrastructure and cyberspace, promote the adoption of AI safety standards globally, reduce the risk of AI’s use to create weapons of mass destruction, combat AI-related intellectual property theft, and ensure our immigration system attracts talent to develop responsible AI in the United States,” Secretary of Homeland Security Alejandro Mayorkas said in a statement. (ctd.)



The plan tasks Mayorkas, who established the Department's AI Task Force in April 2023 and appointed the department's first chief AI officer, with chairing the AI Safety and Security Advisory Board. DHS already uses AI in agency operations like stopping online child sex abuse, fentanyl interdiction and assessing damage after disasters.

In addition, the White House chief of staff and the National Security Council are directed to develop a national security memorandum to ensure the

military and the intelligence community use AI safely, effectively and ethically in their missions.

In addition, the secretary of defense, along with the secretary of veterans affairs and the secretary of health and human services are required to establish an HHS AI task force and develop a plan for responsible use of AI in the health and human services sector, including drug and device safety, research, health care delivery and financing. (ctd.)

Heather Frase

Senior Fellow of AI Assessment at
Georgetown University's Center for
Security and Emerging Technology



“If the White House and executive branch achieve even half of the provisions, it will be a vital step forward to safeguard AI,” Heather Frase, senior fellow of AI assessment at Georgetown University’s Center for Security and Emerging Technology, told GovCIO Media and Research. “The next step beyond developing domestic standards and protections is ensuring that our allies and other countries around the world also adopt similar norms to enable interoperability and the benefits of AI — I’m hopeful that the UK AI Summit and other multilateral efforts like the G7 will carry forward the EO’s momentum.”

Executive Action is Not the Final Word

While the executive order has significant power, legislation will be required to regulate the technology.

“This executive order represents bold action, but we still need Congress to act,” Biden said.

Sen. Mark Warner, chairman of the Senate Select Committee on Intelligence and co-chair of the Senate Cybersecurity Caucus, said some of the provisions “just scratch the surface.”

“I am impressed by the breadth of this Executive Order — with sections devoted to increasing AI workforce inside and outside of government, federal procurement and global engagement. I am also happy to see a number of sections that closely align with my efforts around AI safety and security and federal government’s use of AI,” Warner said.

“At the same time, many of these just scratch the surface — particularly in areas like health care and competition policy. Other areas overlap pending bipartisan legislation, such as the provision related to national security use of AI, which duplicates some of the work in the past two Intel Authorization Acts related to AI governance. While this is a good step forward, we need additional legislative measures,” he added.

Rep. Don Beyer, vice chair of the bipartisan Congressional AI Caucus, said

“If the White House and executive branch achieve even half of the provisions, it will be a vital step forward to safeguard AI. ... The next step beyond developing domestic standards and protections is ensuring that our allies and other countries around the world also adopt similar norms to enable interoperability and the benefits of AI.”

Heather Frase, Senior Fellow of AI Assessment at Georgetown University's Center for Security and Emerging Technology



that legislation is necessary to develop standards for safe and secure AI.

“President Biden’s Executive Order on AI is an ambitiously comprehensive strategy for responsible innovation that builds on previous efforts, including voluntary commitments from leading companies, to ensure the safe, secure

and trustworthy development of AI,” Beyer said in a statement. “We know, however, that there are limits to what the executive branch can do on its own and in the long term, it is necessary for Congress to step up and legislate strong standards for equity, bias, risk management and consumer protection.” ❁

Key Goals of the Cybersecurity Executive Order

As cyber threats evolve, agencies need to prevent, disrupt and mitigate attacks. Signed in 2021, the **White House Executive Order on Improving the Nation's Cybersecurity** outlined a more comprehensive approach to securing networks, requiring agencies to shift toward stronger cyber standards and to adopt advanced security solutions.

IMPLEMENT STRONGER AND MORE MODERN CYBERSECURITY STANDARDS

The plan moves agencies toward secure cloud services and zero-trust architectures. It also mandates multifactor authentication and encryption.

IMPROVE SOFTWARE SUPPLY CHAIN SECURITY

Begin a pilot program to create a label so the public can determine whether software was developed securely and establishes base security standards for development of software sold to the government.

CREATE A CYBER SAFETY REVIEW BOARD

The EO establishes a Cyber Safety Review Board, modeled after the National Transportation Safety Board, that is cochaired by public and private sector officials. The board has the authority to convene following a serious cyber incident to analyze what happened and make recommendations.

ESTABLISH A PLAYBOOK FOR RESPONDING TO CYBER VULNERABILITIES AND INCIDENTS

The order creates a standardized playbook and set of definitions for cyber vulnerability incident response by federal departments and agencies.

REMOVE BARRIERS TO THREAT INFORMATION SHARING

The White House order ensures that service providers can share information with agencies and requires private providers to share breach information.

BETTER DEVELOP INVESTIGATIVE AND REMEDIATION CYBER CAPABILITIES

The plan establishes cyber breach log requirements for agencies to improve the ability to detect intrusions, mitigate those in progress and determine the extent of an incident after the fact.






U.S. Government Solutions



Executive Orders' Impact on Tech Modernization

 What are some of the challenges you've seen arise as agencies are working to meet executive orders and having to modernize their IT infrastructure at the same time?

Padin Over the last four years, we've seen a complete change in mindset about the way our government adapts to new and constantly changing cybersecurity threats. Instead of our traditional approach of creating a five-year plan for modernizing our systems, recent executive orders such as "Improving the Nation's Cybersecurity" and "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" have put a stake in the ground with detailed guidance and a deadline to achieve specific zero trust security goals by the end of fiscal year 2024.


Given the tight deadlines set by the mandates, we've been incredibly impressed by how the administration and all the federal IT leadership have responded with a focused mindset on enhancing cybersecurity and protecting our national security while continuing to modernize the government's essential systems.

That creates a challenge for agencies to develop plans, implement strategies and find quick wins in the short term to find areas to reduce the attack surface. For many

Jose Padin
Chief Transformation
Officer, U.S. Public
Sector, Zscaler



agencies, the biggest challenge to achieving measurable success is the budget. Even though these executive orders established clear policies, there was not clear budget guidance to enable agencies to adapt and implement the necessary changes.

 **What are some successes or use cases where you've seen the executive orders make the impact they intended to make?**

Padin We have a continuous pattern of cybersecurity events across every sector of our society where we see the same pattern. There is an external attack

surface that is exposed and penetrated. Some type of exploit is delivered within a supposedly secure network. Once it's delivered, it moves laterally, does whatever it wants, gets data out, or spills onto the website.

The mandate created by the executive orders has allowed agencies to accelerate and validate the changes in cybersecurity approaches that were already in motion in many agencies in many areas. This has allowed them to adapt more quickly to technologies and tools, and incorporate them into a consolidated plan to achieve the measurements established by the executive orders.

Agencies are recognizing the risk of placing users on a network which allows

“The mandate created by the executive orders has allowed agencies to accelerate and validate the changes in cybersecurity approaches that were already in motion in many agencies...and has allowed them to adapt quickly to technologies and tools and aggregate them into a consolidated plan to achieve the measurements established by the executive orders.”

Jose Padin, Chief Transformation Officer, U.S. Public Sector, Zscaler




lateral movement, which can allow unauthorized users access to critical information. By requiring all users to be authenticated, authorized and continuously validated for security configuration and posture before being granted or keeping access to applications and data, agencies can greatly reduce the risk of attacks.

How does the AI executive order play within agencies' efforts to improve cybersecurity?

Padin Artificial intelligence (AI) and machine learning (ML) are tools. If you think about what our agencies do, there are billions of transactions in seconds within our systems.

AI and ML allow us to aggregate tons of data and see what's going on without human intervention. These tools will allow us to understand large data sets, look for anomalies and then use this understanding to make continuous improvements in cybersecurity. These are necessary technologies that offer real advantages to agencies that can apply them properly.

But AI and ML also can be used maliciously in creating dynamic exploits that can be customized down to specific areas that make it hard to detect. This brings us back to the importance of reducing the risk to your attack surface.

That means that our best opportunities to deter AI and ML-created exploits force us to employ AI and ML to understand the anomalies within our huge data sets so that they can be quickly mitigated. 



Secure. Simplify. Transform.

Protect your agency with the most accredited security cloud in the world. FedRAMP Moderate and High, DoD IL5 and StateRAMP authorized.

- Protect data from cyberthreats
- Reduce IT cost and complexity
- Improve user experience
- Meet mandates with confidence

Learn more at
zscaler.com/federal

Customer Experience Tech Improvements Highlight Biden Executive Order

Agencies are integrating human-centered design principles to improve customer-facing digital platforms and align with the executive order.

A 2021 executive order requires agencies to integrate human-centered design and digital service concepts to improve government's customer experience in areas impacting various stages of the public's lives.

"Americans expect government services to be responsive to their needs," the order said. 'Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government.' "The executive order directs federal agencies to put people at the center of everything the government does."

The order comes on the heels of the President's Management Agenda, which outlines improvements to the customer experience as one of three major objectives, and signifies how the administration is prioritizing technology investments for improving government services.

The directive outlines 36 customer experience improvement commitments across 17 federal agencies, as well as 35 "high-impact service providers" that are charged with improving their digital services.

It calls on the Department of Veterans Affairs (VA), for example, to modernize its veteran-facing digital services to streamline access to health information and reduce redundancies. This includes incorporating login.gov, a cross-agency solution pioneered by the General Services Administration, to remove duplicative sign-on options for access to VA.gov. Additionally, VA is to build out a single,



integrated and fully inclusive digital platform on VA.gov and a flagship VA mobile application to provide additional access opportunities that meet users where they are.

This will be just the latest in a string of efforts the agency — and government overall — has undertaken in recent years for largescale tech modernization.

Since launching the new VA.gov website in 2018, the VA has made strides in

Barbara Morton

Deputy Chief Veterans Experience Officer, Department of Veterans Affairs



placing technology at the center of its mission. VA has leveraged human-centered design concepts across numerous efforts around the veteran experience.

“We wanted to continue to apply the human-centered design methodology and mindset as part of the strategy to redesign the website,” Barbara Morton, VA’s deputy chief veterans experience officer, said during a GovCIO Media & Research’s virtual event in 2021. “When you see it today, you will see a much more user-friendly website ... and you are designing and iterating all the way to the users.”

Biden’s order also urges for improved tools and resources for recipients of Medicare and Medicaid. It calls for the Centers of Medicare and Medicaid Services to roll out personalized online tools for Medicare recipients that will help them save money on medication, manage their health care, access extra customer support and streamline Social Security enrollment.

This is part of what the order calls out as areas to improve technology throughout moments that matter most in people’s lives, like retirement or applying for a small business loan.

Other health-focused agencies have been prioritizing changes to technology that improves the patient experience. This has resonated most in areas like electronic health records modernization, particularly in data storage and access like the efforts at VA.

One callout from the order for continued support is in telehealth capabilities, which falls in line with the numerous investments some agencies have made over the course of the pandemic.

“Patients will have increased ability to use telehealth with their doctors, connecting rural Americans, individuals with disabilities, or individuals seeking the convenience of remote options with the health care they need,” the order said. 🌟

“We wanted to continue to apply the human-centered design methodology and mindset as part of the strategy to redesign the website. When you see it today, you will see a much more user-friendly website ... and you are designing and iterating all the way to the users.”

**—Barbara Morton, Deputy Chief Veterans Experience Officer,
Department of Veterans Affairs**

The CAIOs Leading Responsible AI Development Across Government

Since the White House’s AI executive order was released, federal agencies are in the process of naming chief artificial intelligence officers.

Federal agencies are appointing new chief artificial intelligence officers as part of the collective movement to meet directives set forth from the White House’s AI executive order that tasked agencies with a series of responsibilities connected to the emerging technology.

Although artificial intelligence development in the federal government is not new, this marks the first time federal agencies are all mandated to appoint a designated CAIO, whose responsibilities include “coordinating their agency’s use of AI, promoting AI innovation, [and] managing risks from the use of AI,” according to OMB guidance on AI governance.

Some agencies, like the departments of Health and Human Services, had AI chiefs in place already comprising various forms of the CAIO title.

Department of Agriculture

USDA Chief Data Officer Chris Alvares is responsible for “developing strategies that enable USDA to fully leverage its data as a strategic asset, improving organizational decision-making and outcomes for citizens.”

Defense Department

Craig Martell serves as chief of the Chief Digital and AI Office (CDAO). Martell is also chair of the CDAO Council, leading policy officials and stakeholders in advising leadership, developing strategy and policy, and using data to drive culture within DOD.

Department of Education

Vijay Sharma is Education’s CAIO, where he will fulfill the responsible AI roles set out by the White House. Sharma has served as the department’s chief technology officer since 2015, according to LinkedIn. (ctd.)





Department of Energy

Helena Fu serves as the CAIO for Energy and the director of the newly created Office of Critical and Emerging Technology within the department. Fu will “coordinate the department’s use of

AI, manage risks from its use, and promote innovation,” according to a December agency release.

Department of Health and Human Services

HHS CAIO Greg Singleton has held the position since 2022. Singleton stepped into a role that has existed at the department since March 2021 and is the second person to hold the position — the first being Oki Mek.

Department of Homeland Security

Eric Hysen serves the dual roles of CIO and CAIO for DHS. Hysen was sworn in to the former in 2021 and was named the latter in 2023. Hysen oversees the agency’s acquisition and use of AI, facial recognition applications and promotion of AI innovation and safety within the agency.

Department of Housing and Urban Development

Vinay Singh is HUD’s CFO and CAIO. Singh joined the department in 2022 as CFO after serving as the senior advisor to the administrator at the Small Business Administration. Singh leads the agency’s efforts to use safe and trustworthy AI and promotes innovation and risk management within the department.

Department of Justice

DOJ announced that it named Jonathan Mayer to the dual-hat roles of chief science and technology advisor and CAIO at the department. Mayer is an assistant professor at Princeton University’s Department of Computer Science and School of Public and International Affairs.

Social Security Administration

The Social Security Administration (SSA) named Brian Peltier as acting CAIO. Peltier already serves as SSA’s chief architect and responsible AI official and has been at the agency for almost 20 years. (ctd.)

Department of State

Matthew Graviss serves as the Department of State's chief data and artificial intelligence officer, where he is "responsible for making data accessible, interoperable, and actionable across the Department of State."

General Services Administration

Zach Whitman, who joined GSA in July 2023 as the agency's chief data scientist, assumed the CAIO role in November 2023.

Department of Veterans Affairs

Department of Veterans Affairs CTO Charles Worthington serves as the chief artificial intelligence officer at VA. He recently briefed the House of Representatives on the department's plans to integrate AI into its operations. Additionally, Gil Alterovitz serves as CAIO of the VHA and the director of the National Artificial Intelligence Institute (NAII). He was one of the major players behind the White House's Blueprint for an AI Bill of Rights that preceded the AI executive order.

National Science Foundation

NSF Chief Data Officer and previous CIO Dorothy Aronson now serves as the agency's CAIO. Aronson is in charge of "spearheading strategic initiatives, overseeing AI implementations, and driving innovation," according to an agency spokesperson.

Department of Labor

Louis Charlier has been tapped as DOL's CAIO, the department confirmed to GovCIO Media & Research. Charlier served as the agency's deputy CIO and already had been serving as its responsible AI official.

