

Home • Careers • What the White House executive order on AI means for cybersecurity leaders



by **Christopher Burgess**
Contributing Writer

What the White House executive order on AI means for cybersecurity leaders

Opinion

Oct 31, 2023 • 6 mins

CSO and CISO

Cybercrime

Generative AI

in

CSO



Credit: WH.gov

Artificial intelligence continues to snare the technological limelight and, rightly so as we move well into the final quarter of 2023, there is wide international interest in harnessing the power of AI. But with the excitement and anticipation come some appropriate notes of caution from governments around the world, concerned that all of AI's promise and potential has a dark flipside: It can be used as a tool by bad actors just as easily as it can by the good guys.

Thus, on October 30, 2023, US President Joe Biden issued the "[Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence](#)" while contemporaneously the [G-7 Leaders issued a joint statement](#) in support of the May 2023 "Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems." The US executive order also references the anticipated November [UK Summit on AI Safety](#), which will bring together world leaders, technology companies and AI experts to "facilitate a critical conversation on artificial intelligence."

Understanding how AI will affect the CISO's role is key

Amid the cacophony of international voices trying to bring order to what many see as chaos, it is important for CISOs to understand how AI and machine learning are going to affect their role and their abilities to thwart, detect, and remediate threats. Knowing what the new policy moves entail is critical to gauging where responsibility for dealing with the threats will lie and provides insight into what these governmental bodies believe is the way forward.

CISOs will be well served to ensure they have visibility into the various working groups and advisory boards (e.g., AISSB) as they support their entity's evolution and adoption of AI/ML tools. In addition, given the fluid nature of the global initiatives, the lack of harmonization across borders is a reality and could cause downstream compliance issues if guidance and regulations differ within regions or by country.

This ad will end in 32

The US executive order on AI

The US executive order builds on prior White House engagement on AI and provides guidelines for industry and the government. Those entities that have a national security footprint should be especially attentive to the dual-use possibilities of AI technologies. The executive order points to seven important areas:

1. Ensure safety and security.
2. Protect the privacy of Americans.
3. Advance equity and civil rights.
4. Stand up for consumers and workers.
5. Promote innovation and competition.
6. Advance American leadership abroad.
7. Ensure responsible and effective government use of AI.

Government agencies on the front lines of AI regulation

The National Institute of Standards and Technology (NIST) has a herculean task, which it characterized as an "opportunity" on social media: "AI provides tremendous opportunity, but we also must manage the risks. The [executive order] directs NIST to develop guidelines & best practices to promote consensus industry standards that help ensure the development & deployment of safe, secure & trustworthy AI."

Meanwhile, the White House Office of the National Cyber Director characterized its understanding of the executive order on social media with precision: "Today's EO establishes new standards for AI safety and security, the protection of Americans' privacy, the advancement of equity and civil rights — it stands up for consumers and workers, promotes innovation & competition, advances American leadership around the world."

The US Department of Homeland Security put out its own fact sheet explaining the executive order and its responsibilities, highlighting key areas:

1. Formation of the AI Safety and Security Advisory Board (AISSB) to "support the responsible development of AI. This committee will bring together preeminent industry experts from AI hardware and software companies, leading research labs, critical infrastructure entities, and the U.S. government."
2. Work to develop AI safety and security guidance for use by critical infrastructure owners and operators.
3. Capitalize on AI's potential to improve U.S. cyber defense, highlighting how CISA is actively "leveraging AI and machine learning (ML) tools for threat detection, prevention, vulnerability assessments."

Separately, the Cybersecurity and Infrastructure Security Agency emphasized in its own social media post that it will "assess possible risks related to the use of AI, provide guidance to the critical infrastructure sectors, capitalize on AI's potential to improve US cyber defenses, and develop recommendations for red-teaming generative AI."

Assessing the AI threat to intellectual property

The threat to intellectual property is not hypothetical and is front and center within the executive order. To bolster the protection of AI-related intellectual property, DHS, through the National Intellectual Property Rights Coordination Center "will create a program to help AI developers mitigate AI-related risk, leveraging Homeland Security Investigations, law enforcement, and industry partnerships.

While industry, in the form of IBM, chimed in with the admonishment that the "best way to address potential AI safety concerns is through open innovation. A robust open-source ecosystem with a diversity of voices — including creators, developers, and academics — will help rapidly advance the science of AI safety and foster competition in the marketplace."

It's now been a year since ChatGPT stormed into consumer hands and the past 12 months have been nothing short of whirlwind adoption. CISOs must, as recommended previously, ask the hard questions, and demand provenance and demonstratable test results from providers who espouse the inclusion of AI/ML in their products. While the global government initiatives are pointed in the right direction, it's clear that it will ultimately fall on the CISO's shoulders to determine if the arrows in their quiver are the right ones.



by **Christopher Burgess**
Contributing Writer




Christopher Burgess is a writer, speaker and commentator on security issues. He is a former senior security advisor to Cisco, and has also been a CEO/COO with various startups in the data and security spaces. He served 30+ years within the CIA which awarded him the Distinguished Career Intelligence Medal upon his retirement. Cisco gave him a stetson and a bottle of single-barrel Jack upon his retirement. Christopher co-authored the book, "Secrets Stolen, Fortunes Lost, Preventing Intellectual Property Theft and Economic Espionage in the 21st Century". He also founded the non-profit, Senior Online Safety.

More from this author



Most popular authors

 **Shweta Sharma**
Senior Writer

 **Josh Fruhlinger**
Contributing writer

Cynthia Brumfield
Contributing Writer

Show me more

Popular Articles Podcasts Videos

01

News

Third Wave Innovations rolls security into all-in-one NOC offering

By Jon Gold

Oct 31, 2023 • 3 mins

Threat and Vulnerability Management

Network Security

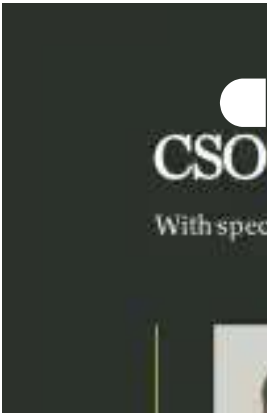
02

Podcast

CSO Executive Sessions Australia with R

Oct 16, 2023 • 15 mins

CSO and CISO



Sponsored Links

Tomorrow's cybersecurity success starts with next-level innovation today. Join the discussion now to sharpen your focus on risk and resilience.

Unified identity security is the new imperative. SailPoint has the roadmap for success - Learn more

About ⌵

About Us

Advertise

Contact Us

Foundry Careers

Reprints

Newsletters

Brandposts

Policies ⌵

Privacy Policy

Cookie Policy

Copyright Notice

Member Preferences

About AdChoices

E-commerce Links

Your California Privacy Rights

Privacy Settings

Our Network ⌵

CIO

Computerworld

Infoworld

Network World