POLSINELLI | What a law firm should be.™

Unpacking the Executive Order on AI (for Cybersecurity)

The race to leverage the digital transformation potential for generative artificial intelligence (AI) has reached fever-pitch levels that began last November with the release of ChatGPT. The fast rise of emerging technologies often leads to the 'slow your roll' development of legal and compliance obligations, sometimes welcomed and sometimes despised.

On Monday, the Whitehouse released its **Executive Order** on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO). The EO and its sixty-four pages will be dissected for weeks, and months given its multiple deadlines. So, what do you need to know, right now?

- **Nothing new impacts businesses *right now*.** The EO does not, in itself, establish any new rules, regulations or reporting requirements for businesses.
- **But new requirements are coming…eventually.** The EO establishes obligations for multiple agencies, ranging from orders to hire and train more AI specialists to due dates on reports and impact assessments. Several include directives to draft, within the next three to twelve months, reporting requirements, regulations, policies and industry standards. Many of these proposals will have to traverse the long and winding road of the rule-making process.
- **Compliance is not Cybersecurity.** The EO is, understandably, reactionary. It is responding to concerns surrounding AI that many businesses should already be actively addressing, such as safety, privacy and perhaps most critically, cybersecurity. The EO's reactive nature highlights the urgency to address AI concerns now. Consult with a trusted legal counsel.

In line with Microsoft's Chief of Security's statement last year that "cybersecurity is the mother of all problems. If you don't solve it, all the other technology stuff just doesn't happen," the EO places a heavy emphasis on cybersecurity, stating in the accompanying Fact Sheet that standards, tools and tests must be developed to address AI systems' cybersecurity risks.

For good reason. Already, organizations have experienced AI-enabled cyberattacks that involved the exfiltration of confidential business information, proprietary information, and source code. These risks, along with the rise of "adversarial" A.I. – the practice of modifying A.I. systems to intentionally manipulate or attack – are just the tip of the iceberg.

To counter these new cybersecurity threats, the EO is requiring the establishment of an advanced cybersecurity program to develop AI tools to find and fix vulnerabilities in critical software. The EO sets forth deadlines by which certain standards must be established for the sharing of information. For example:

- **Cybersecurity Reporting -- Within 90 Days (~January 28, 2024)** – The Secretary of Commerce shall issue reporting requirements for companies developing "dual-use foundation models" to report on when testing of those models will occur, the physical and cybersecurity protections in place for those tests, and the results of those tests. *See* § 4.2(a)-(b).
- **Cybersecurity Record-keeping -- Within 90 Days (~January 28, 2024)** – The Secretary of Commerce shall propose regulations for foreign nationals who train AI with capabilities to be used in malicious cyber-enabled activities to register and maintain certain record-keeping functions before having access to United States Infrastructure as a Service ("IaaS"). *See* § 4.2(c).
- **Critical Infrastructure Guidelines -- Within 180 Days (~March 28, 2024)** – The Secretary of Homeland Security will incorporate AI risks into relevant safety and security guidelines for use by critical infrastructure owners and operators. *See* § 4.3(a).

While the EO is primarily aimed at federal agencies and AI developers, AI's risks underscore the need for **all** organizations to revisit their cybersecurity posture, especially their incident response plans, to conduct risk assessments, and maintain security programs. All of these are already generally mandated as legal, regulatory, or industry standards.

Save the Date

- November 15: Polsinelli will unpack the EO's public policy and data privacy implications.
- December 7: Polsinelli will commence an AI webinar series, 'Emerging Legal Concepts with Generative AI in 2024'. Register **now**.
- In the first quarter of 2024, lawyers from Polsinelli's healthcare, intellectual property, labor and employment, and data privacy and cybersecurity groups will provide relevant guidance.

For other recent content addressing AI, see Polsinelli alerts titled ***Chatbots: Select Legal Considerations for Businesses***, and ***Artificial Intelligence Has a NIST Framework for Cybersecurity Risk***, and **Generative AI's 'Industry Standards' for Cybersecurity and Data Privacy Could be Here Sooner Rather than Later.**