October 5, 2022

TLP White

This week, Hacking Healthcare begins by breaking down a new notice from the U.S. Treasury Department that requests feedback on the potential need for a federal cyber insurance response to significant cyber incidents, especially those that hit critical infrastructure. Following that, we briefly examine the Biden administration's blueprint for an A.I. Bill of Rights and how its impact may be limited.

Welcome back to *Hacking Healthcare*.

1. **Treasury Opens Up for Comments on Potential Federal Cyber Insurance**

   With all manner of malicious cyberattacks seemingly becoming commonplace, the continued and unfortunate targeting of critical infrastructure sectors like healthcare and public health leads to questions as to whether governments should be doing more to help protect organizations from attacks and to help them recover. While some have advocated for more aggressive and offensive minded approaches, the U.S. Department of the Treasury has been assessing the role of the federal government as it relates to cyber insurance. The Treasury Department is now looking for comments to help shape its understanding of the issue.

   Within this environment, the Government Accountability Office (GAO) conducted a report to assess the "cyber risks to U.S. critical infrastructure and available insurance for these risks." That report, which was published back in June, found that cyber insurance does indeed help offset the costs associated with common cyber risks, but that those risks are growing, and critical infrastructure sectors are increasingly being targeted by increasingly more severe attacks.[1]

   On September 29, the Treasury Department published a Request for Comment (RFC) seeking public input on a wide range of issues related to cyber insurance that will feed into a joint assessment being conducted by the Federal Insurance Office (FIO)[2] within Treasury and the Cybersecurity and Infrastructure Security Agency (CISA).[3] The comments will help shape how CISA and FIO go about assessing "the extent to which

risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response."[4]

Specifically, the RFC asks questions within the categories of *Catastrophic Cyber Incidents* and *Potential Federal Insurance Response for Catastrophic Cyber Incidents*, as described below.

Catastrophic Cyber Incidents: This section asks for comments related to the nature of a catastrophic cyber event, what kinds of methodologies could be used to assess or measure financial and insured loss, and what sorts of cybersecurity measures would most effectively reduce either the likelihood or scale of cyber incidents. Additionally, it asks what the federal government could do to incentivize or require cyber insurance policy holders to adopt such measures.

Potential Federal Insurance Response for Catastrophic Cyber Incidents: This section is considerably longer and seeks comments on a wider range of issues. It includes questions to assess the current cyber insurance coverage environment, what kinds of private sector information might be shareable with the government, whether the private sector thinks a federal insurance response is warranted, how such a response might be structured, who should be required to participate in such a response, how to reduce the moral hazard of introducing such a response, and several other issues.

Additionally, the RFC invites any other additional comments or information that broadly relate to the issue. Those interested in responding will have until November 14 to submit comments for consideration.

Action and Analysis
Membership required

2. Biden Administration Releases A.I. Bill of Rights Blueprint

On October 4, the Biden administration's Office of Science and Technology Policy (OSTP) published a vision for how automated systems can be leveraged without threatening to exacerbate inequality, biases, threats to democracy, or any other of myriad potential ills. The document fills the glaring gap of policy guidance that many other Western nations have already laid down.[5]

The OSTP described the blueprint as the product of an extensive consultative process that received input from "impacted communities and industry stakeholders to technology developers and other experts across fields and sectors, as well as policymakers throughout the Federal government."[6] At its core, the document sets out "five principles and associated practices to help guide the design, use, and deployment

of automated systems to protect the rights of the American public in the age of artificial intelligence."[7]

The five principles are:

- Safe and effective systems
- Algorithmic discrimination protections
- Data privacy
- Notice and explanation
- Human alternatives, consideration, and fallback

Action and Analysis
Membership required

Congress

Tuesday, October 4th:
- No relevant hearings

Wednesday, October 5th:
- No relevant hearings

Thursday, October 6th:
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

Friday, October 7th:
Personal Data Sharing – Emerging Technologies (ENISA)

Monday, October 10th:
- 7th eHealth Security Conference (ENISA)

Conferences, Webinars, and Summits

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

About the Author

Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

---

[1] https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents

2 The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) established the Federal Insurance Office (FIO) within the U.S. Department of the Treasury. Among their responsibilities, they monitor all aspects of the insurance industry, including identifying issues or gaps in the regulation of insurers that could contribute to a systemic crisis in the insurance industry or the U.S. financial system

[3] https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents

[4] https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents

[5] https://www.technologyreview.com/2022/10/04/1060600/white-house-ai-bill-of-rights/

[6] https://www.whitehouse.gov/ostp/ai-bill-of-rights/what-is-the-blueprint-for-an-ai-bill-of-rights/

[7] https://www.whitehouse.gov/ostp/ai-bill-of-rights/what-is-the-blueprint-for-an-ai-bill-of-rights/