HACKING HEALTHCARE™

Health-ISAC Weekly Blog -- Hacking Healthcare™

TLP:WHITE

May 02, 2024

This week, *Hacking Healthcare*™ Focuses on new developments around AI risk, safety, and security. In particular, we breakdown the establishment of the new Department of Homeland Security (DHS) Artificial Intelligence Safety and Security Board and then review new DHS guidance Safety and Security Guidelines for Critical Infrastructure Owners and Operators.

Welcome back to *Hacking Healthcare*™.

Health-ISAC Americas Hobby Exercise 2024
The Health-ISAC is once again ramping up preparations for our annual Americas Hobby Exercise! For new Health-ISAC members, the Hobby Exercise is an annual Healthcare and Public Health (HPH) event designed to engage the healthcare sector and strategic partners on significant security and resilience challenges. The overarching objective is to inform and provide opportunities for organizational continuous improvement while increasing healthcare sector resiliency.

The following link to last year's Hobby Exercise After Action Report provides a good overview of the kinds of interaction and value you can expect from this year's event:
https://h-isac.org/hobby-exercise-2023-after-action-report/

This year's exercise will be held on June 6 at Venable LLPs office in Washington, D.C. Members are encouraged to register their interest in participation at the following link: https://portal.h-isac.org/s/community-event?id=a1Y7V00000ZmFVwUAN

New DHS AI Safety and Security Board

The Biden administration published Executive Order (E.O.) 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, in October 2023.[i] As a follow-on action from that EO, DHS published a notice in the Federal Register on Monday April 29th notifying the public of their establishment of the Artificial Intelligence Safety and Security Board.[ii]

But what is this board? Who is on it? What are they empowered to do? How might it affect the healthcare and public health (HPH) sector?

What is their mission?

Established through the Office of Partnership and Engagement, the board will "advise the Secretary [of DHS], the critical infrastructure community, other private sector stakeholders, and the broader public on the safe and secure development and deployment of AI technology in our nation's critical infrastructure."[iii] Furthermore, the board is to provide the Secretary of DHS with "advice, and recommendations to advance the security and resilience" of Critical infrastructure's use of AI.[iv]

What is the scope of work and what authorities do they have?

The full scope of activities is not defined, but the Federal Register notice outlines that they may include "information about emergent risks, threat mitigation guidance, and guardrails for critical infrastructure owners' and operators' use of AI."[v] In terms of authorities, the board is only to act in an advisory capacity. Notably, the board has been exempted from the The Federal Advisory Committee Act (FACA). This exemption was granted by the Secretary of DHS "In recognition of the sensitive nature of the subject matter involved."[vi] More on that in the Action & Analysis section.

Who are its members?

According to the Federal Register notice, the board's membership may consist of up to 35 representative members and the Secretary of DHS. The various board members are appointed by and serve at the pleasure of the Secretary of DHS and serve terms of two years. The board membership is instructed to be "diverse with regard to

professional and technical expertise," and "shall include AI experts from the private sector, academia, and government, as appropriate."[vii]
As of April 26th, DHS has announced that in addition to the secretary, 22 individuals have been selected. These include prominent individuals and organizations such as:

- Sam Altman, CEO, OpenAI;
- Jensen Huang, President and CEO, NVIDIA;
- Sundar Pichai, CEO, Alphabet;
- Wes Moore, Governor of Maryland;
- Alexandra Reeve Givens, President and CEO, Center for Democracy and Technology
- Ed Bastian, CEO, Delta Air Lines; and
- Chuck Robbins, Chair and CEO, Cisco; Chair, Business Roundtable.

What are its initial priorities?
According to DHS' press release, the board will meet for the first time early next month and will meet quarterly after that. The initial priorities for the board have been outlined as:[viii]

- Provide the Secretary and the critical infrastructure community with actionable recommendations to ensure the safe adoption of AI technology in the essential services Americans depend upon every day
- Create a forum for DHS, the critical infrastructure community, and AI leaders to share information on the security risks presented by AI.

We will dig a bit deeper into what to expect from this group in the *Action & Analysis* section, but let's first jump to a related news item…

New DHS AI Safety and Security Guidelines for Critical Infrastructure
In yet another action tied to EO 14110, on April 29, DHS released "new resources to address threats posed by AI," that included "guidelines to mitigate AI risks to critical infrastructure."[ix] The new guidelines are published in a 28-page document, Safety and Security Guidelines for Critical Infrastructure Owners and Operators, that is

organized to address three “overarching categories of system-level risk”:[x]

- Attacks Using AI: The use of AI to enhance, plan, or scale physical attacks on, or cyber compromises of, critical infrastructure.
- Attacks Targeting AI Systems: Targeted attacks on AI systems supporting critical infrastructure.
- Failures in AI Design and Implementation: Deficiencies or inadequacies in the planning, structure, implementation, or execution of an AI tool or system leading to malfunctions or other unintended consequences that affect critical infrastructure operations.

The guidelines were developed in partnership with various government agencies that included the “Department of Commerce, the Sector Risk Management Agencies (SRMAs) for the 16 critical infrastructure sectors, and relevant independent regulatory agencies.”[xi]

Contents

The first half of the document is used to outline AI risks to critical infrastructure, potential beneficial uses of AI, and four categories of guidelines for critical infrastructure owners and operators. These four categories address actions organizations should take to help mitigate AI risk:[xii]

- **Govern**: Which seeks to “support the establishment of policies, processes, and procedures to anticipate, identify, and manage the benefits and risks of AI at all points in the AI lifecycle.”
- **Map**: Which seeks to “establish the foundational context from which owners and operators of critical infrastructure can evaluate and mitigate AI risks.”
- **Measure**: Which seeks to “identify repeatable methods and metrics for measuring and monitoring AI risks and impacts throughout the AI system lifecycle”
- **Manage**: Which seeks to “define risk management controls and best practices for implementing and maintaining them to increase the benefits of AI systems while decreasing the likelihood of harmful safety and security impacts.”

The second half of the document, in the form of two appendices, outline cross-sector AI risks and mitigation strategies in a general way and also map the guidelines above to the NIST AI Risk Management Framework (RMF).[xiii]

Action & Analysis
Included with Health-ISAC Membership

Upcoming International Hearings/Meetings

- EU

No relevant meetings at this time

- US

No relevant meetings at this time

- Rest of World

No relevant meetings at this time

[i] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/
[ii] https://www.federalregister.gov/documents/2024/04/29/2024-09132/establishment-of-the-artificial-intelligence-safety-and-security-board
[iii] https://www.dhs.gov/news/2024/04/26/over-20-technology-and-critical-infrastructure-executives-civil-rights-leaders
[iv] https://www.federalregister.gov/documents/2024/04/29/2024-09132/establishment-of-the-artificial-intelligence-safety-and-security-board
[v] https://www.federalregister.gov/documents/2024/04/29/2024-09132/establishment-of-the-artificial-intelligence-safety-and-security-board
[vi] https://www.federalregister.gov/documents/2024/04/29/2024-09132/establishment-of-the-artificial-intelligence-safety-and-security-board
[vii] https://www.federalregister.gov/documents/2024/04/29/2024-09132/establishment-of-the-artificial-intelligence-safety-and-security-board

[viii] https://www.dhs.gov/news/2024/04/26/over-20-technology-and-critical-infrastructure-executives-civil-rights-leaders
[ix] https://www.dhs.gov/news/2024/04/29/dhs-publishes-guidelines-and-report-secure-critical-infrastructure-and-weapons-mass
[x] https://www.dhs.gov/news/2024/04/29/dhs-publishes-guidelines-and-report-secure-critical-infrastructure-and-weapons-mass
[xi] https://www.dhs.gov/publication/safety-and-security-guidelines-critical-infrastructure-owners-and-operators
[xii] https://www.dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf
[xiii] https://www.nist.gov/itl/ai-risk-management-framework
[xiv] https://www.gsa.gov/policy-regulations/policy/federal-advisory-committee-management
[xv] OpenAI, Anthropic, NVIDIA, IBM, Microsoft, Adobe, Alphabet, Amazon Web Services, and AMD
[xvi] Humane Intelligence, Center for Democracy and Technology, Lawyers' Committee for Civil Rights Under Law, Stanford Human-centered Artificial Intelligence Institute, Brookings Institution, The Leadership Conference on Civil and Human Rights
[xvii] https://www.cisa.gov/resources-tools/resources/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer-2023

Report Source(s)	Health-ISAC

Release Date
May 03, 2024 (UTC)

Alert ID 45fa024d

View Alert

Tags Safety and Security Guidelines for Critical Infrastructure Owners and Operators, Artificial Intelligence Safety and Security Board, AI Risk, Artificial Intelligence

Hacking Healthcare™

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has 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.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC's annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC's monthly Threat Briefing.

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

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**