Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare | TLP:WHITE | Alert ID : 709b576a | Jan 18, 2024, 02:11 PM

This week, *Hacking Healthcare*™ begins by taking a look at a range of new cooperative agreements between the U.S. and the E.U. We provide some broader geopolitical context and break down how some of the recent developments may directly and indirectly affect the healthcare sector.

Welcome back to *Hacking Healthcare*™.

New U.S.-E.U Cyber & Tech Cooperation

In the past few weeks, the U.S. and E.U. have made progress on several initiatives aimed at increasing cooperation and reciprocity on various cyber and technology matters. These initiatives are an encouraging sign that the two entities are strengthening needed partnerships despite some differences in governance and strategy. So, what are these new initiatives that will help tackle global cyber threats and streamline the international regulatory landscape?

CISA & ENISA Working Arrangement

It may have flown under the radar as we approached the year's end and the holiday season, but in early December, representatives from the U.S. and E.U. met for the 9th E.U.-U.S. Cyber Dialogue in Belgium. At the meeting, the U.S. and E.U., "reaffirmed their continued commitment to an open, free, interoperable, secure, and reliable Internet, respecting human rights and fundamental freedoms" and "committed to advancing international security and stability in cyberspace…"[i] In addition, they exchanged policy views on a range of cyber topics and highlighted concerns about cyber threats to supply chains, critical infrastructure, and the continued menace of ransomware.

One of the more significant accomplishments of the dialog was the formalization of a Working Arrangement between the U.S.' Cybersecurity and Infrastructure Security Agency (CISA) and the E.U.'s Cybersecurity Agency (ENISA). The ENISA announcement detailed that this new arrangement will "[consolidate] present areas of cooperation, as well as [open] the door to new ones."[ii]

Specifically, ENISA highlighted the following areas for focus:[iii]

- **Cyber awareness & capacity building to enhance cyber resilience**: "including facilitating the participation as third country representatives in specific EU-wide cybersecurity exercises or trainings and the sharing and promotion of cyber awareness tools and programmes."

- **Best-practice exchange in the implementation of cyber legislation**: "including on key cyber legislation implementation such as the NIS Directive, incident reporting, vulnerabilities management and the approach to sectors such as telecommunications and energy**."**

- **Knowledge and information sharing to increase common situational awareness**: "including a more systematic sharing of knowledge and information in relation to the cybersecurity threat landscape to increase the common situational awareness to the stakeholders and communities and in full respect of data protection requirements."

A plan to operationalize these focus areas is an expected next step, and representatives of the E.U. and U.S. will meet again for the tenth annual U.S.-E.U. Cyber Dialogue in Washington, DC later this year.

Cybersecurity Labeling Reciprocity

Another issue area where positive progress appears to have recently been made between the U.S. and E.U. is in cybersecurity labeling. Both entities have been pursuing labeling approaches that would help consumers and end users understand the cybersecurity of devices.

According to reports from last week, the U.S. and E.U. have made progress on a working agreement that would allow reciprocity between the eventual U.S. IoT and E.U. cybersecurity labeling schemes. Speaking at the Consumer Electronics Show, U.S. National Security Council official Anne Neuberger highlighted the desire to ensure that passing certification in one jurisdiction will allow a product or device to be placed on the market in the other without additional burdens.[iv]

Action & Analysis
Included with Health-ISAC Membership

Congress
Tuesday, January 16
No relevant hearings

Wednesday, January 17
No relevant meetings

Thursday, January 18
No relevant meetings

International Hearings/Meetings
No relevant meetings
EU

[i] https://www.state.gov/joint-statement-on-the-united-states-european-union-9th-cyber-dialogue-in-brussels/
[ii] https://www.enisa.europa.eu/news/cisa-and-enisa-enhance-their-cooperation
[iii] https://www.enisa.europa.eu/news/cisa-and-enisa-enhance-their-cooperation
[iv] https://insidecybersecurity.com/daily-news/white-house-establishes-partnership-european-union-rolling-out-internet-things-labeling
[v] https://www.fcc.gov/consumer-governmental-affairs/fcc-proposes-cybersecurity-labeling-program-smart-devices
[vi] https://www.state.gov/joint-statement-on-the-united-states-european-union-9th-cyber-dialogue-in-brussels/
[vii] https://www.state.gov/joint-statement-on-the-united-states-european-union-9th-cyber-dialogue-in-brussels/

Report Source(s)

Health-ISAC

Reference | References

state
insidecybersecurity
Europa Analytics
fcc

Tags

CRA, Hacking Healthcare, Information Sharing, CISA, law, European Union

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

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

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.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org