April 13th, 2021

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins by exploring the role of the United States National Cyber Director, including the role’s origins, what one in the role is expected to do, its international equivalents, and how it might impact the healthcare sector. Next, we briefly summarize the impact of a major U.S. Supreme Court decision on a dispute between Google and Oracle over APIs. Lastly, we provide an overview of the European Union Agency for Cybersecurity’s (ENISA) new online tool, which is connected to the hospital cybersecurity procurement guidelines they released last year. Welcome back to *Hacking Healthcare*.

1. **The United States National Cyber Director**

   As with any policy area, each U.S. presidential administration over the past few decades has set their specific cyber policy approach and has nominated or appointed personnel to facilitate it. Because the cyber domain has increasingly grown in importance, more recent presidential administrations have taken to creating positions that are specifically tailored to the cybersecurity space. This includes President Bush’s creation of the ”Special Advisor to the President on Cybersecurity” role and President Obama’s “National Cybersecurity Coordinator,” a role that was eliminated without replacement under President Trump.

   The common theme of the past three administrations is that there has been no specific executive position, let alone an office with supporting personnel, that was mandated to exist to tackle and coordinate cyber issues. That changed with Congress’ passage of last year’s National Defense Authorization Act (NDAA).

   The NDAA is a complex law that “provides authorization of appropriations for the Department of Defense (DOD)..., DOD elements of the Intelligence Community, and defense-related activities at other federal agencies.”[1] It is an enormous piece of legislation that has been passed for 60 consecutive years, making it the closest thing to a guarantee in the U.S. Congress.

   Last year’s NDAA, which passed with strong bi-partisan support, included the establishment of the United States National Cyber Director (NCD), as well as the Office of the National Cyber Director (ONCD) to support the position. In essence, Congress now requires there to be a presidentially nominated and Senate approved individual who will serve as the principal advisor to the President on cybersecurity policy, strategy, and for coordinating cyber efforts across government.

NCD responsibilities will include advising U.S. agencies, leading policy and strategy implementation, leading coordinated response efforts to cyberattacks, engaging with the private sector, and issuing rules and regulations. Creating such a high-level position within the Executive Office of the President goes a long way towards formally recognizing the elevated importance of the cyber domain, as well as the advantage that comes with having some institutional coherence between presidential administrations and across federal agencies when it comes to cybersecurity.

This type of role is not entirely unique across the globe. Some states, such as Australia and New Zealand, have Cyber Ambassadors that cover more of the ceremonial and public-facing responsibilities of the NCD. Other states, such as Singapore, make the head of their national cyber agency the de facto leader of their cyber policy strategy. So, while the NCD may be uniquely configured for the US system of governance, its general role and responsibilities can be found in various positions in other states.

With expectations that Biden will soon formally nominate Chris Inglis for the senate confirmation process, we may not have to wait much longer to see how this position begins to take shape.

Action & Analysis
H-ISAC Membership Required

2. Google Beats Oracle in Biggest Programming Copyright Supreme Court Case Ever

After 10 years of legal drama between Oracle and Google, the Supreme Court of the United States (SCOTUS) issued a decision that application programming interfaces (APIs) fall under the fair use doctrine, thereby siding with Google in a copyright lawsuit. For those not familiar with software programming, APIs are intermediaries that allow different software or applications to “speak” with each other. APIs define functions and are used in a variety of coding environments from web design to iPhone apps to transferring medical records. Since APIs are widely used, the recent SCOTUS decision will have significant consequences throughout software development and programming, including in the healthcare space.

In Google LLC v. Oracle America, Inc., Oracle argued that Google infringed on Oracle’s copyright by using 37 Java APIs and 11,500 lines of Java code in their Android OS. Google’s counter argument was that an API is just a building block, not something covered by a copyright. Throughout the last decade, there have been many decisions at varying levels of the U.S. court system addressing different pieces of this case. The case was tried before two District Court juries and the U.S. Court of Appeals for the Federal Circuit before being granted certiorari by SCOTUS.

After hearing the arguments on the case in 2020, this month SCOTUS ruled that Google could legally use Oracle's API code when building Android, stating that "Google's copying of the API to reimplement a user interface, taking only what was needed to allow users to put their accrued talents to work in a new and transformative program, constituted a fair use of that material" in the decision.[2] This 2021 decision overturned a previous lower federal court ruling that held in favor of Oracle.

Even though SCOTUS sided with Google in this most recent case, the decision is more nuanced than simply saying Google was correct and APIs cannot be copyrighted. SCOTUS specifically stated that "to decide no more than is necessary to resolve this case, the Court assumes for argument's sake that the copied lines can be copyrighted, and focuses on whether Google's use of those lines was a 'fair use.'"[3] The idea that the Java APIs were "fair use" aligns with industry practices. Microsoft agreed in an amicus filing that sharing and modifying code to create new products and functions is a common practice among programmers and that drawing from function code is required for sound development.

Action & Analysis
H-ISAC Membership Required

3. Procurement Guidelines for Cybersecurity in Hospitals: New Online Tool for a Customized Experience

Last year, ENISA released *Procurement Guidelines for Cybersecurity in Hospitals*.[4] The guide highlighted the importance of securing every aspect of the healthcare information and communication technology ecosystem, emphasizing the sometimes-overlooked procurement step, and strived to provide a comprehensive set of practices that can be adapted to fit hospitals' procurement processes. The 51-page guidance counted C-suite level executives, IT professionals, and procurement officers as the target audience and was narrowly focused on the hospital environment, but much of the guidance and recommendations are applicable throughout the healthcare sector.

Fast forward a year and ENISA has now released a companion tool to *Procurement Guidelines for Cybersecurity in Hospitals* with the goal of helping "healthcare organisations identify best practices in order to meet cybersecurity needs when procuring products or services."[5] The new, web-based tool was developed to be a complement to the procurement guidelines and hopes to help healthcare organizations quickly identify the parts of the guidelines that are most relevant to their organization and promote appropriate security measures.[6] Additionally, ENISA published a concise version of the procurement guidelines in all 22 official EU languages.[7] The web tool came about due to stakeholder input that recommended an interactive format for the guidelines so that users can customize searches and boost their decision making.

The new web tool includes tailored best practice recommendations for procurement of building management systems, clinical information systems, cloud services, identification systems, industrial control systems, medical devices, mobile client devices, network equipment, professional services, and remote care systems.[8] The tailored best practices include details on which threats a specific action can help mitigate. The tool also includes many filtering options, making it easy for a user to get a broad overview or dive deep into a specialized problem – making this a handy link to bookmark if you operate in the EU. Given that *Procurement Guidelines for Cybersecurity in Hospitals* was well-received due to its accessible and non-technical writing style, this even more accessible, complementing tool should be welcomed by organizations with business units in the EU.

As hospitals and other organizations look to grow and expand their offerings, procurement is a key process that can shape that ecosystem, making it more important than ever that cybersecurity is considered at the beginning of the procurement process, not at the end or as an afterthought. Organizations may wish to assess this ENISA tool's applicability to current processes, as it may help to fill gaps or expedite current practices.

Congress –

Tuesday, April 13th:
- No relevant hearings

Wednesday, April 14th:
- No relevant hearings

Thursday, April 15th:
- Senate – Committee on Commerce, Science, and Transportation – subcommittee on Communication, Media, and Broadband: Hearings to examine communicating trusted vaccine information.

- Senate – Committee on Finance: Hearings to examine the nominations of Andrea Joan Palm, of Wisconsin, to be Deputy Secretary, and Chiquita Brooks-LaSure, of Virginia, to be Administrator of the Centers for Medicare and Medicaid Service, both of the Department of Health and Human Services.

- House – Committee on Appropriations – Subcommittee on the Departments of Labor, Health and Human Services, Education, and Related Agencies: FY 2022 Budget Request for the Department of Health and Human Services

International Hearings/Meetings –

- No relevant hearings

EU –

Thursday, April 15th:

- European Parliament – Committee on the Environment, Public Health and Food Safety: A reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices / Commission Delegated Regulation amending Regulation (EC) No 1234/2008 concerning the examination of variations to the terms of marketing authorisations for medicinal products for human use and veterinary medicinal products

Conferences, Webinars, and Summits –

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

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

[1] https://fas.org/sgp/crs/natsec/IF10515.pdf

[2] https://www.zdnet.com/article/google-beats-oracle-in-biggest-programming-copyright-supreme-court-case-ever/

[3] https://www.zdnet.com/article/google-beats-oracle-in-biggest-programming-copyright-supreme-court-case-ever/

[4] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[5] https://www.enisa.europa.eu/news/enisa-news/procurement-guidelines-for-cybersecurity-in-hospitals-new-online-tool-for-a-customised-experience

[6] https://www.enisa.europa.eu/news/enisa-news/procurement-guidelines-for-cybersecurity-in-hospitals-new-online-tool-for-a-customised-experience

[7] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[8] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health/good-practices-for-the-security-of-healthcare-services#/