



TLP White

This week, *Hacking Healthcare* examines Singapore's 2018 Cybersecurity Act. In particular, we breakdown what their "light-weight" licensing framework will mean for healthcare organizations that employ penetration testing and managed security operations centers. We then evaluate a new legislative bill introduced in the United States Senate that would require the Department of Homeland Security (DHS) to share cybersecurity information with legislative bodies more quickly. We take a look at how this legislation could impact the private sector organizations that share sensitive information, like technical indicators, with government entities.

Welcome back to *Hacking Healthcare*.

1. Singapore Cybersecurity Act Effect on Penetration Testing and Managed Security Operations Centers

Singapore has been a leader in the Asia-Pacific region for technology and cybersecurity policy in recent years. Their *2018 Cybersecurity Act* was meant to establish "a legal framework for the oversight and maintenance of national cybersecurity in Singapore."¹ Among its four pillars was the development of a licensing framework for cybersecurity service providers. While the bill might have been passed four-years ago, this section is just now coming into effect, and it may have ramifications for healthcare sector organizations operating in the country.

The Cybersecurity Act received the Singaporean President's assent back in March of 2018, but the date of Commencement for some parts of the Act didn't come into effect until last Monday.² At the time of the legislation's creation, there were four objectives sought by legislators:³

- Strengthen the protection of Critical Information Infrastructure (CII) against cyber-attacks

April 19, 2022

- Authorize the Cyber Security Agency of Singapore (CSA) to prevent and respond to cybersecurity threats and incidents
- Establish a framework for sharing cybersecurity information
- Establish a light-touch licensing framework for cybersecurity service providers

The establishment of a licensing framework for cybersecurity service providers is initially scoped to two specific services: penetration testing and managed security operations centers (SOCs). These two were chosen because of the sensitive information they create and/or have access to, and because they are “relatively mainstream in [Singapore’s] market.” The intent was to find a framework that struck a balance “between security needs and the development of a vibrant cybersecurity ecosystem.”⁴

So, what does the licensing framework do? In effect, to provide or advertise any of the cybersecurity services covered by the law (penetration testing & SOCs), a person or organization must first obtain a license through the Singapore Government’s Cybersecurity Services Regulation Office (CSRO). Failure to do so could result in fines of up to \$50,000 and/or two-years in prison.⁵

The Cybersecurity Act 2018 outlines the terms and conditions for being granted a license, including meeting fit and proper criteria, and the requiring that licensees keep detailed records of each time it provides licensed services. Additionally, it lays out the terms by which a license can be revoked or suspended and the financial penalties for violations.

For businesses, an application costs roughly \$731 USD at the time of this writing, with individual license half of that.⁶ Furthermore, any applications received prior to April of next year are 50% off. Each License will also last two years from the date of issuance, which the CSRO says will take no more than 6 weeks to process once submitted.⁷

Action & Analysis

Membership required

2. Bill Introduced to Increase Cybersecurity Sharing Between DHS and Congress

Keeping with the theme of potential unintended consequences, we note that earlier this month a bipartisan bill was introduced in the United States Senate that would require increased information sharing between the DHS and Congress. However, there may be a significant gap between what the authors of the bill reportedly want it to do, and what it may end up doing if it is signed into law. Furthermore, there are some concerns with

April 19, 2022

how private sector information may end up trickling into this proposed sharing agreement.

The *Intragovernmental Cybersecurity Information Sharing Act* is reportedly a response to the delays that congressional lawmakers feel they face in receiving “information on cybersecurity threats from the Executive Branch.”^{8,9} In their eyes, this disconnect hinders a “unified and coordinated defense”, and that actionable cybersecurity information should be sent to the Sergeant at Arms of the Senate and the Chief Administrative Officer of the House of Representatives, so that their respective institutions can be better protected.¹⁰ For those not familiar with the roles and responsibilities of the United State’s legislative branch, the Sergeant at Arms of the Senate and the Chief Administrative Officer of the House of Representatives each have responsibilities relating to the day to day operations and security of the their respective institutions.

In particular, the bill would require that the Secretary of Homeland Security enter into one or more “cybersecurity information sharing agreements with the Sergeant at Arms and Doorkeeper of the Senate, and the Chief Administrative Officer of the House of Representatives to ensure robust collaboration between the executive branch and Congress on Federal cybersecurity.”¹¹ However, the content of these agreements is not defined.

The bill only lays out that the parties involved will work together to develop appropriate elements. These may include:¹²

- Direct and timely sharing of technical indicators and contextual information on cyber threats and vulnerabilities;
- Direct and timely sharing of classified and unclassified reports on cyber threats and activities; and
- Seating of cybersecurity personnel of the Senate or the House of Representatives at cybersecurity operations centers.

Action & Analysis

****Membership required****

April 19, 2022

Congress

Tuesday, April 19th:

- No relevant hearings

Wednesday, April 20th:

- No relevant hearings

Thursday, April 21st:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

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, and 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.csa.gov.sg/legislation/cybersecurity-act>

April 19, 2022

² <https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312&WholeDoc=1>

³ <https://www.csa.gov.sg/legislation/cybersecurity-act>

⁴ <https://www.csa.gov.sg/legislation/cybersecurity-act>

⁵ <https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312&WholeDoc=1&Provs=pr24-,pr25-,pr26-,pr27-,pr28-,pr29-,pr30-,pr31-,pr32-,pr33-,pr34-,pr35->

⁶ <https://www.csro.gov.sg/how-to/apply-for-licence>

⁷ <https://www.csro.gov.sg/how-to/apply-for-licence>

⁸ <https://www.congress.gov/bill/117th-congress/senate-bill/4000/text?q=%7B%22search%22%3A%5B%22%5C%22cybersecurity+information+sharing+act%5C%22%22%2C%22%5C%22cybersecurity%22%2C%22information%22%2C%22sharing%22%2C%22act%5C%22%22%5D%7D&r=1&s=5>

⁹ <https://www.hsgac.senate.gov/media/minority-media/portman-klobuchar-blunt-peters-introduce-bipartisan-legislation-to-ensure-congressional-cybersecurity-defenders-receive-timely-cybersecurity-information>

¹⁰ <https://www.meritalk.com/articles/senate-bill-aims-to-speed-cyber-info-sharing-between-congress-administration/>

¹¹ <https://www.congress.gov/bill/117th-congress/senate-bill/4000/text?q=%7B%22search%22%3A%5B%22%5C%22cybersecurity+information+sharing+act%5C%22%22%2C%22%5C%22cybersecurity%22%2C%22information%22%2C%22sharing%22%2C%22act%5C%22%22%5D%7D&r=1&s=5>

¹² <https://www.congress.gov/bill/117th-congress/senate-bill/4000/text?q=%7B%22search%22%3A%5B%22%5C%22cybersecurity+information+sharing+act%5C%22%22%2C%22%5C%22cybersecurity%22%2C%22information%22%2C%22sharing%22%2C%22act%5C%22%22%5D%7D&r=1&s=5>