August 23, 2022

TLP White

This week, Hacking Healthcare begins by examining a new Department of Homeland Security Report that tasks the Cybersecurity and Infrastructure Security Agency (CISA) with doing more to improve their cyber information sharing with private sector partners. Next, we play six degrees of separation as we show how Janet Jackson relates to cyber resiliency. No, really. Welcome back to *Hacking Healthcare*.

1. **DHS Inspector General Tells CISA to Improve Information Sharing**

   Information sharing remains one of the most important aspects of cybersecurity, but many private sector organizations have been critical of how quickly, accurately, and comprehensively important information has trickled down from governmental entities. A recent report from the Department of Homeland Security's (DHS) Office of Inspector General (OIG) gives credence to some of those complaints as they relate to the Cybersecurity and Infrastructure Security Agency (CISA).

   For those unfamiliar with the OIG, the office came into being the same time as DHS in 2002, and is led by a senate-confirmed inspector general who is tasked with "[providing] independent oversight and [promoting] excellence, integrity, and accountability within the DHS."[1] The report published last Tuesday is bluntly titled *Additional Progress Needed to Improve Information Sharing under the Cybersecurity Act of 2015*, and its 36 pages contain "four recommendations aimed at improving information sharing."[2] Notably, the report makes clear that CISA concurred with the initial findings of the OIG's draft report on this matter, and the OIG has recognized that three of the recommendations have been acted upon and are resolved, while one remains unresolved.

   So, what were the identified information sharing failures?

   The OIG report concluded that while CISA has "addressed the basic information sharing requirements of the Cybersecurity Act of 2015," they have made "limited progress improving the overall quality of threat information."[3] The OIG found that the lack of quality "was not always adequate to identify and mitigate cyber threats," and that "most of the cyber threat indicators did not contain enough contextual information to help decision makers take action."[4] The report additionally concluded that this issue

negatively impacted private sector entities and "may hinder the Federal Government's ability to identify and mitigate potential cyber vulnerabilities and threats."[5]

The OIG ultimately determined there were several causes for these issues:[6]

> Limited Automated Indicator Sharing (AIS) functionality: AIS was a capability created 6 years ago to "enable the real-time exchange of unclassified cyber threat information and defensive measures." However, the OIG noted that "AIS contains a limited number of fields and attributes that can be used by participants sharing cyber threat information," and that "some fields that would provide more contextual information for each cyber threat indicator were restricted or not required."
>
> Insufficient staffing: The OIG found that "DHS leadership has not funded nor dedicated an adequate number of full-time employees to this effort."
>
> External factors: The report found a mix of external factors that included a failure among some federal entities to adhere to using "access control specification markings to identify shared cyber threat indicators," a lack of internal staff and resources at smaller federal entities and private sector entities to "share cyber threat indicators;" and a "reluctance" of some federal entities to share information outside of some "communities," such as international entities.

From these identified issues, the OIG presented the following recommendations:[7]

> Recommendation 1: We recommend the Director of CISA develop and implement a formal process to verify the number of cyber threat indicators and defensive measures shared through CISA's Automated Indicator Sharing capabilities in order to enable accurate reporting and oversight.
>
> Recommendation 2: We recommend the Director of CISA develop and implement an approach to encourage Federal agencies and the private sector to comply with information sharing agreements and requirements, and report actions taken with information sharing agreements and requirements for Automated Indicator Sharing.
>
> Recommendation 3: We recommend the Director of CISA complete Automated Indicator Sharing (AIS) 2.0 upgrades.
>
> Recommendation 4: We recommend the Director of CISA place priority on hiring administrative and operational staffing to conduct the strategic planning, coordination, analysis, and performance measurement needed to mitigate cybersecurity risks.

These recommendations were present in an earlier draft report provided to CISA, who concurred with all four recommendations, and had at the time of the OIG final report resolved two of the four recommendations fully.

According to the final report, OIG is satisfied that CISA has taken the necessary steps to address recommendations two and three; however, questions remain on

recommendations one and four. CISA reports have vaguely added additional resources to support recommendation four, and plans on assessing the allocation of more, but they currently don't anticipate that being completed before January 31, 2023. Recommendation one also appears problematic with the OIG reporting that CISA's actions are "not responsive to this recommendation."[8]

Action & Analysis
*Included with H-ISAC Members

2. **What Janet Jackson Can Teach Us About Cyber Resiliency**

   In what is one of the more eyebrow-raising cybersecurity news stories of the year, "Janet Jackson's *Rhythm Nation* music video of 1989 has officially been declared a security vulnerability."[9] While it is a headline you might expect to read on April Fool's Day, the issue has been assigned an official CVE number and is a very real, albeit limited, vulnerability.[10]

   For the technically minded, the CVE describes the vulnerability as "[allowing] physically proximate attackers to cause a denial of service (device malfunction and system crash) via a resonant-frequency attack." In simpler terms, for a certain make of 5400 RPM OEM hard drive that "shipped with laptop PCs in approximately 2005," the song contains "one of the natural resonant frequencies" that the hard drive uses which interferes with its normal operation.[11, 12]

   The author of the Microsoft blog post that generated much of the interest in this story reports that the issue was addressed by the manufacturer "adding a custom filter in the audio pipeline that detected and removed the offending frequencies during audio playback."[13]

   Action & Analysis
   *Included with H-ISAC Members

Congress -

Tuesday, August 23rd:
- No relevant hearings

Wednesday, August 24th:
- No relevant hearings

Thursday, August 25th:
- No relevant hearings

International Hearings/Meetings -

- No relevant meetings

EU –

- No relevant meetings

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.oig.dhs.gov/about
[2] https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-59-Aug22.pdf
[3] https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-59-Aug22.pdf
[4] https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-59-Aug22.pdf
[5] https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-59-Aug22.pdf
[6] https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-59-Aug22.pdf
[7] https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-59-Aug22.pdf
[8] https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-59-Aug22.pdf
[9] https://www.bleepingcomputer.com/news/security/janet-jacksons-music-video-is-now-a-vulnerability-for-crashing-hard-disks/
[10] https://nvd.nist.gov/vuln/detail/CVE-2022-38392
[11] https://devblogs.microsoft.com/oldnewthing/20220816-00/?p=106994
[12] https://arstechnica.com/gadgets/2022/08/janet-jacksons-rhythm-nation-is-officially-a-security-threat-for-some-old-laptops/
[13] https://devblogs.microsoft.com/oldnewthing/20220816-00/?p=106994