Byers, Dave

From: Byers, Dave
Sent: Monday, September 26, 2022 1:08 PM
To: Kevin Bowling; Stacey Marz
Cc: Slayton, David
Subject: FW: Following up from Center for Internet Security re COSCA-NCSC
Attachments: cisa-advisory-committee-draft-recommendations (Sep 13, 2022).pdf

At our recent JTC meeting, you expressed about contact MS-ISAC to see what more we can do with them. I had a meeting scheduled with Brain today and he has forwarded this info....I think it would be good to schedule a meeting with You two and Brian (I am happy to join) to discuss what more they can do for courts. Let me know if you want me to set it up.

From: Brian de Vallance (Contractor) <Brian.deVallance@cisecurity.org>
Sent: Monday, September 26, 2022 12:01 PM
To: Byers, Dave <DByers@courts.az.gov>
Subject: Following up from Center for Internet Security re COSCA-NCSC

Dave, thanks for the good discussion.

I'm resending the elements from before (below). I love your idea about Sam Thumma or Scott Bales. I know them both well. I'll give you all the credit!

Plus, we're adding:

- Election Security briefing (see the sample from what we presented to the House Homeland Security Committee after the 2020 election) (close hold); and
- State Bar of Arizona: I'm checking whether they can be a member. I would imagine that they could.

I look forward to our discussion with your Joint Tech Committee folks. I know I presented, at your invitation, to them late last year or early this year. And I remember that Mr. Boling was chair or co-chair.

Talk soon.

Thanks.

Brian

From: Brian de Vallance <Brian.deVallance@cisecurity.org>
Date: Thursday, September 15, 2022 at 7:37 AM
To: Dave Byers <DByers@courts.az.gov>, "Kim, Anthony" <aykim@ncsc.org>
Subject: Checking in from Center for Internet Security

Gentlemen, good morning. Randy Rose is traveling and I haven't yet had a chance to connect with him about Monday's JTC national webinar, but thought I'd check in with you to see how it went and whether we can help with anything as follow up.

Related, here are a couple of items that we might want to keep on our ongoing agenda about how CIS can assist NCSC and COSCA on a regular basis. For example:

- **Ransomware Task Force's Blueprint on Ransomware Defense**: The Ransomware Task Force (RTF) just completed this Blueprint last month. It is intended to be a single, authoritative roadmap for small- and midsized organizations to protect against ransomware. CIS is part of the RTF, and the Blueprint's technical backbone was based on CIS's Critical Security Controls. The RTF is briefing Congress, DHS CISA, the new White House Office of National Cyber Director, and some of the SLTT groups. We would be happy to provide a briefing to your JTC or another venue, if helpful. Blueprint here: https://securityandtechnology.org/ransomwaretaskforce/blueprint-for-ransomware-defense/
- **Reasonableness Project**: CIS is also starting a project to help courts and legal counsel determine what constitutes "reasonable security" in cyber cases, a growing field. We are talking to the ABA and others about this perhaps becoming part of their CLE series. We would love to identify a (retired) state judge to help lead the group. I'd love to talk to you about you about who you might think would be a good representative of the bench.
- **Initiative to focus on encouraging those who haven't yet, sign up for the free MS-ISAC.** Perhaps we can do a webinar that provides a deeper dive for IT personnel about how the Multi-State Information Sharing & Analysis Center (MS-ISAC) can help—focused perhaps on the courts that might need to be educated on what we can do for free. I'm imagining the county and various city courts. The MS-ISAC is like the free space in Bingo—you have to play it first.
- **CISA Cybersecurity Advisory Committee recommendation**: At its quarterly meeting yesterday, the Committee was scheduled to present a final version of the two draft reports (attached). In the second report, Information Sharing Around Foreign Adversary Threats to Elections, the Committee makes two recommendations: (1) work with the intelligence community to "ensure that the information needs of election officials around foreign disinformation threats are prioritized"; and (2) **Protect the courts**. The relevant part of the recommendation: Courts "may be the target of an intensified campaign to undermine public trust in the legitimacy of their processes. CISA should consider the following two recommendations that:
  - Relevant information around foreign hacking and disinformation attacks are shared with the courts; and
  - The IC includes adversary activity targeting the courts in the collection and analysis priorities related to elections. With regard to the state and local courts, I recommend that we start a conversation and not wait for CISA to call you guys and us—that we proactively prep and ask for a meeting.

Let me know what you think. Happy to have a short call on any or all of these.

Thank you!

Brian