Draft: 11/16/2022

Cybersecurity (H) Working Group
Virtual Meeting
November 15, 2022

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Oct. 11, 2022. The following Working Group members participated: Cynthia Amann, Co-Chair (MO); Wendy Erdly, Co-Chair (NY); C.J. Metcalf, Co-Vice Chair (IL); Michael Peterson, Co-Vice Chair (VA); Sian Ng-Ashcraft (AK); Chris Erwin (AR); Lance Hirano (HI); Alex Borkowski (MD); Jake Martin (MI); Troy Smith (MO); Martin Swanson (NE); Colton Schulz and Chris Aufenthie (ND); Barbara D. Richardson (NV); Don Layson (OH); Dan Petterson (VT); John Jacobson (WA); and Rachel Cissne Carabell (WI).

1. Adopted its October 11 Meeting Minutes

Schulz made a motion, seconded by Amann to adopt the Working Group's October 11 minutes (Attachment). The motion passed unanimously.

2. Discussed Cybersecurity with the Cybersecurity and Infrastructure Security Agency (CISA)

Erdly led a discussion with CISA's Executive Director, Brandon Wales. The discussion touched on several topics.

Wales said that CISA's work consists of two broad missions. CISA is responsibility for coordinating national efforts around critical infrastructure, security, and resilience. Because CISA is not a part of the law enforcement community or the intelligence community, the organization is purpose built for partnership with industry. The second mission is related to operational responsibility for the security of federal, civilian executive branch networks. CISA provides information, guidance, and technical advisories related to cybersecurity.

Related to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Erdly asked about the act, what makes it important, and how CIRCIA will determine who is critical infrastructure and therefore will be subject to the reporting requirements of the Act. Wales responded that CIRCIA will help the federal government have better visibility to cybersecurity trends noting that currently the federal government estimates that it only knows about 20 to 30% of the cyber attacks that hit the United States which prevents the government from providing early warning to additional victims which further allows campaigns to spread more quickly. Therefore the law now requires incident reporting with CISA working on what will qualify as a covered incident who will qualify as a covered entity. CISA wants to make sure that when they issue their final rule to apply the authority given to them in CIRCIA, that result in a clear definition allowing members of industry to understand whether they qualify as critical infrastructure or not. Lastly, CISA also wants to make sure that they are receiving the most relevant information for covered incidents understanding that incidents evolve quickly and that limited information may be available at times. Erdly asked further about the type of information CISA anticipates gathering with Wales responding that the information will be of the sort that helps CISA advise the rest of the community about emerging threats including information on tactics and techniques used by adversaries. Erdly asked if the incident information CISA gathers could be shared with state insurance regulators. Wales responded that there are restrictions in how information can be used, for instance criminal proceedings, and so there may be information they have to remove for privacy reasons, but that CISA anticipates being able to share information with state insurance regulators. Miguel Romero (NAIC) asked if CISA anticipated taking an active aiding in the investigation of cybersecurity incidents or passive role largely focused on gathering information. Wales responded that CISA's role can vary based on what is needed but that generally they expect to gather information when working with industry representatives. Romero asked if the information gathered would include consumer level information.

Wales responded that given CISA's focus on protecting all companies, consumer level information may not be relevant.

Erdly next asked about CISA's Cybersecurity Performance Goals. Erdly indicated that the goals originate from a National Security Memorandum signed by President Biden on July 2021. The memorandum required that CISA work with the National Institute of Standards of Technology (NIST) to develop baseline cybersecurity performance goals that are consistent across all critical infrastructure. The goals are a voluntary set of cybersecurity practices intended to help those deemed to be critical infrastructure, especially small and medium sized organizations. Wales added that the goals were developed with industry input and that the goals are a focused set of controls most essential to achieving positive cybersecurity outcomes. They draw on the NIST Cybersecurity Framework (CSF), but don't cover every practice referenced in the CSF. The goals also include insights on the anticipated cost and complexity of implementation so organizations can evaluate their own capacity as they decide which controls to implement.

Erdly next asked how state insurance regulators can support CISA's work. Wales talked about the importance of having sound due diligence related to cybersecurity insurance underwriting because he views cyber insurance as a really critical mechanism to improve cybersecurity risk mitigation. Wales further indicated that the Department of Treasury is studying at the possibility of a federal backstop for cyber insurance.

Erdly next asked about CISA's Shield's Up Program. Wales indicated that the program originated in 2021 as the US government recognized that Russia was likely to invade Ukraine and that there may be implications for US cybersecurity based on the US's support for Ukraine. The program recommends a series of steps a company should take to mitigate risk possibly as a reprisal from Russia. Suggested practices include using multi-factor authentication on administrative accounts and segmenting networks as much as possible. The program also suggests other practices for instance lowering the threshold for reporting incidents to governmental agencies and making sure the company has adequate equipment for operations in case of supply chain issues.

3. <u>Discussed Other Matters</u>

Having no further business, the Cybersecurity (H) Working Group adjourned.

Https://naiconline.sharepoint.com/sites/NAICSupportStaffHub/Member Meetings/H CMTE/2022_Fall/Cybersecurity/C(H)WG 11-15-2022 Minutes.docx