NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Date: 5/9/2024

Virtual Meeting

INFORMATION TECHNOLOGY (IT) EXAMINATION (E) WORKING GROUP
Thursday, May 9, 2024
2:00-3:00 p.m. ET / 1:00-2:00 p.m. CT / 12:00-1:00 p.m. MT / 11:00 a.m.-12:00 p.m. PT

ROLL CALL

Ber Vang, Chair	California	Kim Dobbs/Cynthia Amann	Missouri
Shane Mead, Vice-Chair	Kansas	Lindsay Crawford	Nebraska
Blase Abreo	Alabama	Eileen Fox	New York
Mel Anderson	Arkansas	Colton Schulz	North Dakota
Ken Roulier/Michael Shanahan	Connecticut	Metty Nyangoro	Ohio
Ginny Godek	Illinois	Eli Snowbarger	Oklahoma
Jerry Ehlers	Indiana	Diana Sherman	Pennsylvania
Dmitriy Valekha	Maryland		

NAIC Support Staff: Jacob Steilen

AGENDA

1. Discuss Activities in Response to March 7, 2023, Referral from the Cybersecurity (H) Working Group—*Shane Mead (KS)* Attachment 1

2. Receive Update on National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0—*Colton Schulz (ND)*

3. Discuss Drafting Group Goals for 2024—*Ber Vang (CA)*

4. Discuss Any Other Matters Brought Before the Working Group —*Ber Vang (CA)*

5. Adjournment

IT Exam Working Group - Drafting Group Memo

2023 Drafting Group Activities:

The drafting group met 2 times throughout 2023 to address a referral received from the Cybersecurity (E) Working Group. During these calls, the drafting group accomplished the following:

- Decided there could be a benefit to prioritizing more cybersecurity risks as part of the IT examination.
    - However, the conclusions reached regarding cybersecurity risks and the current IT General Controls conclusion would have to be separated due to timing and the differences in subject matter.

- Reviewed possible sources of guidance to help implement additional cybersecurity guidance, including:
    - NIST (National Institute of Standards and Technology) Framework 2.0
    - CIS (Center of Internet Security)
    - CPGs (Cross-sector baseline cybersecurity goals)
    - Cybersecurity codes of conduct
    - Cybersecurity scoring tools
    - International resources/Issue papers
    - Other Sources

- Selected the NIST framework as the primary resource for updating the guidance based on the following criteria:
    - The NIST framework is formatted similar to Exhibit C, which would ease the integration process and reduce overlap.
    - The new NIST guidance, with its on cybersecurity governance, introduced several concepts not currently represented in Exhibit C.

- Targeted areas of Exhibit C that were redundant, obsolete, or would possibly overlap with the new NIST guidance.
    - Eliminating guidance in these areas would improve the efficiency of the Exhibit C process.
    - The eliminated guidance would also allow cybersecurity concepts to be added without increasing the overall workload required to complete the IT review.

NATIONAL ASSOCIATION OF
INSURANCE COMMISSIONERS

MEMORANDUM

TO: Jerry Ehlers, Chair, Information Technology (IT) Examination (E) Working Group
Ber Vang, Vice-Chair, Information Technology (IT) Examination (E) Working Group

FROM: Cindy Amann, Co-Chair, Cybersecurity (H) Working Group
Wendy Erldy, Co-Chair, Cybersecurity (H) Working Group
CJ Metcalf, Co-Vice-Chair, Cybersecurity (H) Working Group
Michael Peterson, Co-Vice-Chair, Cybersecurity (H) Working Group

DATE: March 7, 2023

RE: Cybersecurity Procedures

The Cybersecurity (H) Working Group has several charges that call on the working group to monitor industry trends and to coordinate our work with the IT Examination (E) Working Group. Those include:

A. Monitor cybersecurity trends such as vulnerabilities, risk management, governance practices, and breaches with the potential to affect the insurance industry.
E. Monitor federal and international activities on cybersecurity engaging on efforts to manage and evaluate cybersecurity risk.
F. Coordinate NAIC committee cybersecurity work, including cybersecurity guidance developed by the Market Conduct Examination Guidelines (D) Working Group and the Information Technology (IT) Examination (E) Working Group.

In keeping with those charges, the Cybersecurity (H) Working Group met with the Executive Director from the Cybersecurity and Infrastructure Security Agency (CISA), Brandon Wales, who provided an update on his agency's work. As part of the update, Mr. Wales mentioned his agency's work to develop and publish a "Cross-Sector Baseline Cybersecurity Performance Goals (CPGs)". Per CISA's website, "the CPGs are a prioritized subset of IT and operational technology (OT) cybersecurity practices that critical infrastructure owners and operators can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques."

More importantly, these CPG's the Cybersecurity (H) Working Group is suggesting this publication to the IT Examination (E) Working Group as it may represent an opportunity to update the cybersecurity related guidance contained within the *Financial Condition Examiners Handbook* (Handbook). While the guidance in the Handbook has long served regulators as an effective tool to investigate a myriad of risks, cybersecurity included, this tool or other resources may represent an opportunity to ensure the work program appropriately prioritizes cybersecurity related considerations.

Therefore, the Cybersecurity (H) Working Group asks the IT Examination (E) Working Group to consider the following:

- Whether the existing guidance would benefit from an update to better prioritize cybersecurity risks.
- If so, whether the CPGs or a different resource (i.e., NIST, CIS, etc.) would aid in a project to update cybersecurity guidance.
    - For instance, the CIS listing of security controls includes a tiering that may make that a useful tool that allows regulators to distinguish relevant controls from key controls.
- Whether any international developments could prove beneficial as a resource towards this project (i.e., Issues Paper under development by the Operational Resilience Task Force).

This is potentially a substantial project, but one that could enhance the regulatory ability to investigate cybersecurity risks. An update may also identify specific procedures that are less relevant as the focus of investigations prioritizes cybersecurity over the review of IT general controls. Upon a quick review by one of our Working Group volunteers, we found substantial overlap between the CPGs and the existing Handbook work program. However, the IT Examination (E) Working Group may find that the CPGs more clearly or simply articulate the controls that are needed to directly address cybersecurity risks. There may also be procedures that while still relevant could be de-emphasized or investigated via inquiry to better allow for cybersecurity to remain a core focus.

The Cybersecurity (H) Working Group acknowledges less ambitious ideas may also be appropriate but stands ready to support the work of the IT Examination (E) Working Group in whatever approach to this project and study is chosen.

Please work with our NAIC support staff, Miguel Romero and Sara Robben to keep our group updated on your progress and decisions.