Insurance Data Security Model Law #668 – Compliance & Enforcement Guide

Introduction

The Insurance Data Security Model Law #668 (IDSM) ~~provides~~ establishes many requirements of affected licensees. The enforcement of compliance is complicated by other, similar efforts across U.S. States' and Territories' departments of insurance, in both their financial and market regulation activities. As such, much of this guidance will focus on the reduction ~~in~~ of the risk of duplicative ~~and redundant~~ work while enforcing compliance with the IDSM.

To reduce the risk of duplicative ~~and redundant~~ work, ~~foreign~~ regulators should generally place reliance on foreign licensees' domestic regulators, especially if they have ~~passed a version of~~adopted the IDSM, to regulate their own market. A method to provide ~~foreign~~ regulators with adequate assurance will leverage Section 4(I) of the IDSM, allowing licensees from IDSM ~~states~~jurisdictions to avoid ~~duplicative and~~ redundant scrutiny. Additionally, provisions for the work of domestic IT examiners to act in lieu of a specific IDSM examination will be discussed, as well as the performance of a gap analysis to maintain alignment among departments.

Attached is a flow diagram providing a decision tree (attachment 1). The idea is to create a process by which IDSM compliance is determined by relying on the work done by other departments, where appropriate, but only from other IDSM ~~states~~jurisdictions. While the work to pass a version of the IDSM in each jurisdiction is ~~not~~ incomplete and ongoing, the final state that this guide envisions is one where each IDSM ~~state~~jurisdiction enforces its law on ~~their~~ its ~~domestics~~ domestic licensees without the need for additional scrutiny by ~~foreign departments~~other jurisdictions in which the licensee operates. With all ~~states~~jurisdictions working together we can create a seamless regulatory environment for our licensees and maximal protection for our consumers.

Objective

The foundational element provided in this guidance is that the domestic regulator has multiple tools available to enforce compliance with the IDSM and should be entrusted to perform that role. This guidance provides an IDSM compliance review processes for the domestic regulator ~~that~~ who focuses on compiling all relevant work and performing a gap analysis ~~between them and~~against the requirements of the IDSM. This approach ensures consistent work across jurisdictions without any ~~duplicative~~ work being redundantly performed by examiners.

Further, using the attestation of compliance to determine a foreign licensee's compliance will allow a more ~~a~~ seamless regulatory environment once the IDSM is ~~passed~~ adopted in all jurisdictions. However, ~~since~~ until an accreditation process for IDSM compliance reviews has ~~not yet~~ been agreed upon, a gap analysis ~~is still~~will be required to determine if any additional inquiry into ~~the~~ a ~~foreign~~ non-domestic department's area of concern is necessary.

Lastly, collaboration among departments is central to the ~~task~~ aim of reducing duplicative ~~and redundant~~ work by ~~foreign~~ non-domestic regulators. By understanding what work was done by the licensee's domestic regulator, the ~~foreign~~ non-domestic regulator's requirements may be fully satisfied. Even if this is not the case, in-depth discussion between domestic and ~~foreign~~ non-domestic regulator will ensure that any action taken by a ~~foreign~~ non-domestic regulator is properly scoped and planned based on the work done to date.

State Collaboration

The IDSM provides a department's Commissioner with broad powers to investigate violations of the IDSM among licensees. This power can be found in the IDSM Section 7, and it applies to all licensees, presuming that there are situations where it is appropriate for a department to perform an examination action on a foreign licensee. This guide notes that this situation could result in substantial duplicative ~~and redundant~~ work and should be first approached collaboratively between departments.

It is possible that a department's concerns may have already been addressed by others during its routine regulatory work. One particularly useful document in the hands of the domestic regulator in an IDSM ~~state~~jurisdiction is the certificate (or affidavit) of compliance required under Section 4(I). For those ~~states~~jurisdictions ~~who~~ that have a mature approach to IDSM regulation, requesting this document may provide all the assurance a ~~foreign~~ non-domestic regulator requires. This is not possible with New York (to be discussed later), but New York domiciled licensees can, themselves, provide a highly similar document that can be similarly leveraged by a ~~foreign~~ non-domestic regulator.

For those situations where a ~~foreign~~ non-domestic regulator requires deeper or additional review from what has already been performed, continued contact is key as the ~~foreign~~ non-domestic regulator performs a gap analysis. As noted in the introduction, the most obvious source of compliance for the IDSM is the IT Review performed at the beginning of a financial condition examination. However, other efforts by the domestic regulator may also provide IDSM assurances. This will be discussed further in the Practical Guidance.

Among the ways to engage with the requirements of the IDSM, effective communication among departments can provide the most robust defense against duplicative ~~or redundant~~ examination work.

Gap Analysis

The gap analysis references a process where one determines if there are any mismatches or gaps between what is being done and what should be done according to a given standard. The reason this step is required is because while IT Reviews are robust ~~that~~ and look deeply into a licensee's IT environment, they are not perfectly aligned with the requirements of the IDSM.

It may be the case that the work done by the IT examiners during a financial condition examination provides everything required for an IDSM Review. However, since this is not necessarily the case, it is incumbent upon the ~~one~~ jurisdiction performing an IDSM Review to confirm that there are no gaps between the IT Review work done and ~~their state's~~that jurisdiction's IDSM.

An important tool in performing a gap analysis is the mapping provided (attachment 2). This will provide the regulator with insight into how to connect Exhibit C to the IDSM, allowing for a shared approach to gap analyses across departments of insurance.

Licensees Regulated Under Health Insurance Portability and Accountability Act (HIPAA)

Section 9(A)(2) of the IDSM discusses HIPAA licensees' ~~their~~ exemption from Section 4 of the IDSM. This document primarily discusses Section 4 compliance and enforcement, which for those licensees who are

regulated under HIPAA, does not apply. The reason is because the Department of Health and Human Services performs such work while determining compliance with HIPAA, and we expect our affected licensees to maintain such compliance. However, while HIPAA licensees are exempt from the requirements of Section 4, they are ~~expected~~ required to provide a separate certificate of compliance (similar to the requirement found in Section 4(I)) certifying HIPAA compliance.

Practical Guidance for Domestic Regulators in IDSM States

The primary regulatory authority for a licensee will be its domestic regulator who has a variety of tools available to determine compliance with the IDSM, most commonly the IT Review. During a financial condition examination by a domestic regulator, an IT Review is regularly performed. The IT Review is robust and generally covers all areas of interest to Section 4 of the IDSM. However, the IT Review is currently based on the COBIT framework, with future improvements focused on the National Institutes of Standards and Technology (NIST) Cybersecurity Framework (CSF), not the IDSM. Fortunately, there is a mapping between COBIT and Section 4 of the IDSM (attachment 2), which provides examiners with the necessary context to understand the work that's been completed. ~~That being said~~Notwithstanding, some jurisdictions will allow for other control frameworks beyond Exhibit C and as such, while this guide is framework agnostic, only a mapping between Exhibit C and the IDSM will be provided.

Commented [SM1]: I don't think this has been established. Only the breakout of cybersecurity controls review into a separate Exhibit C Part Three will use the NIST CSF 2.0 as its framework, while the ITGC review will remain aligned with the COBIT framework but updated to its current version.

Another~~,~~ less common tool~~,~~ available to the domestic regulator is any target examination where the IT function is explored. Much like with the IT Review, ~~it is expected that~~ a target examination's ~~utilizes~~ utilization of the current Exhibit C (COBIT based framework)~~, and~~ can also be mapped to Section 4 of the IDSM. However, ~~for those~~ examinations that investigate areas of IT through other apertures, like the examination of an enterprise risk management program's operational and cybersecurity risk area, may be more challenging to map and care should be taken while doing so.

A focus for departments enforcing the IDSM is the alignment of efforts across divisions (e.g., market & financial regulation), so that the duplication of procedures does not occur. In general, the requirements set forth in Section 4 of the IDSM can be investigated and enforced effectively during an IT Review, but this may not always be the case. To fully determine if a licensee is compliant with the IDSM, a gap analysis should be performed by the domestic ~~state~~ regulator to ensure all applicable measures are in place. Lastly, the guidance to avoid duplication does not ~~preclude~~ prohibit the inclusion of procedures found necessary to investigate any violation of the IDSM (see Section 7), even if similar procedures had been performed during an IT Review or another examination.

Practical Guidance for IDSM States Examining Licensees in ~~Foreign~~ Non-domestic Jurisdictions

There are two categories of licensee of consideration to ~~foreign~~ non-domestic regulators, those that are domesticated in an IDSM ~~state~~jurisdiction and those that are not. Those licensees that are domesticated in IDSM ~~states~~jurisdictions have a unique method by which they can communicate compliance, the annual certification (or affidavit) of compliance required by the IDSM's Section 4(I). Given the robust powers already in possession by the domestic regulator, any ~~foreign~~ non-domestic regulator interested in the IDSM compliance should request this certification first.

The certification required under Section 4(I) requires extensive documentation of any remedial efforts required for the IT environment. Further, it is important to keep in mind that even if remedial actions are

found within the certification, it is incumbent upon the domestic regulator in an IDSM ~~state~~jurisdiction to manage the remediation that's been identified.

Under unusual circumstances, like where a ~~foreign~~ licensee ~~does~~ writes much of its business in ~~the~~ a non-domestic regulator's state, the two departments should first communicate with each other to avoid redundant efforts. It may be the case that the ~~foreign~~ non-domestic regulator is ~~best~~ better suited to perform the work, but this should be done with the knowledge and agreement of the domestic regulator ~~of any~~in the IDSM ~~state~~jurisdiction. Lastly, if a ~~foreign~~ non-domestic regulator is performing IDSM examinations or ~~follow~~ follow-up work for the domestic regulator, care should be taken to avoid duplication and ensure that only one regulator is ultimately responsible.

States without an IDSM usually, but not always, lack a unique method by which they can communicate compliance. Consider the outlier, New York, whose cybersecurity regulation, 23 NYCRR 500, which ~~was what~~ the IDSM was based on, contains exactly the kind of certification of compliance under ~~their~~ 500.17(b) as does Section 4(I) of the IDSM. Given such similarities, this guidance recommends that departments rely on New York's 23 NYCRR 500.17(b) certificate of compliance as they would an IDSM Section 4(I) certificate of compliance. However, ~~there is a wrinkle, because~~ New York's confidentiality responsibilities are ~~not like everyone else's~~unlike those of IDSM jurisdictions, so ~~you'll~~ regulators in IDSM jurisdictions will have to request the compliance certification document from the licensee, not the New York Department of Financial Services.

The remaining jurisdictions, however, do not have as comparable of an artefact as does New York. This does not mean that assurance is not being ~~attained~~obtained, or that work is not being done, further emphasizing the need for communication among departments and for the performance of gap analyses.

At the time of this guide's initial publication, the IDSM has not been adopted across ~~the~~ all U.S. States~~'~~ and Territories~~'~~. As such, consideration for those foreign licensees that are not domesticated in an IDSM ~~state~~jurisdiction must also consider duplication and redundancy of work. As discussed, domestic regulators have the IT Review that covers many or all areas required under the IDSM, and outreach among departments may unveil substantial work necessary for determination of IDSM compliance. Further, other ~~states~~jurisdictions may have their own cybersecurity or privacy laws that, while different than the IDSM, may contain requirements that are suitable. As such, it is important for the ~~foreign~~ non-domestic regulator to reach out and understand the work done by the domestic regulator before utilizing Section 7 of the IDSM.

Examination Considerations

For those situations where a regulator has determined that an IDSM Review (see Section 7) is required, then the two primary considerations are alignment with existing efforts and the maintenance of confidentiality as required by the IDSM's Section 8. Since an objective of this guidance is to create an environment where the domestic regulator can generally be relied upon to enforce the IDSM among ~~their~~ its domestic licensees, the following examination considerations will focus on domestic action. For those rare situations where a ~~foreign~~ regulator ~~from~~ in an IDSM ~~state~~ jurisdiction is examining a ~~non-domestic~~foreign licensee's compliance with ~~their~~ its IDSM, coordination with the licensee's domestic ~~state~~ regulator to address the situation is the recommended first step.

Commented [SM2]: To maintain consistency with the FCEH, the word *foreign* should be applied only to the licensee and not the regulator.

The first task, alignment with existing efforts, asks the domestic regulator to determine what has already been done prior to developing ~~their~~ its work plan. An IDSM Review~~,~~ should take place only after a gap analysis has been completed. The gap analysis, as previously discussed, should take into consideration all sources of compliance, especially including any IT Review or other examination work with a significant IT element. Careful review by the examiner of this work will prevent any unnecessary procedures. The mapping document provided may also prove helpful in this situation, allowing for a clearer alignment of efforts.

The second task, maintaining confidentiality, is addressed by the NAIC's coordinated examination system ~~existing~~ hosted in a highly secure environment that~~, which~~ meets ~~or exceeds the highest~~ the ~~security,~~ confidentiality, integrity, and ~~resilience~~ availability standards ~~in IT~~of FedRAMP Moderate authorization. Further, confidentiality and security standards continue when the targeted examination reports are uploaded to the Financial Examination Electronic Tracking System (FEETS). Departments of insurance already have significant responsibilities when it comes to confidentiality, and leveraging that capability by using the two aforementioned tools will ensure the confidentiality ~~expectation~~ required by Section 8 of the IDSM.

Commented [SM3]: The NAIC coordinated examination database is hosted in a FedRAMP authorized public cloud deployment environment that meets Impact Level - Moderate. There are other security standards and frameworks that exceed FedRAMP standards, including FedRAMP High (for unclassified data), DoD IL5, and ultimately DoD IL6, but FedRAMP Moderate is presumed to be the highest security standard for commercial public SaaS providers.

Regardless, some jurisdictions subscribe to the SOC 2 compliance hosting environment, instead of the FedRAMP environment. The IDSM review files for these states will not have the stated security level.

STATE OF MICHIGAN
GRETCHEN WHITMER
GOVERNOR

DEPARTMENT OF INSURANCE AND FINANCIAL SERVICES
LANSING

ANITA G. FOX
DIRECTOR

September 12, 2025

Transmitted via Email: khenry@naic.org, maromero@naic.org

Koty Henry
Miguel Romero
NAIC Cybersecurity Working Group

Re: Comments regarding the CFRF Referral Response and the associated IDSM Compliance Guide

Dear Mr. Henry and Mr. Romero,

The Michigan Department of Insurance and Financial Services' (DIFS) has reviewed the CFRF Referral Response and the associated IDSM Compliance Guide and appreciates the opportunity to respond to the draft proposals. DIFS would also like to express our thanks to the states involved in drafting the proposals. Please see the following comments which reflect our questions and concerns regarding the proposed drafts.

CFRF Referral Response

- Regarding the cybersecurity breach repository, how does the working group envision the repository synchronizing with the IDSM Compliance Guide? It may be prudent to explain this in the CFRF Referral Response.
- We recommend spelling out acronyms in the Memorandum for additional clarity.

IDSM Compliance Guide

- DIFS has concerns related to shifting the burden from insurance companies to the domestic state relative to cybersecurity incidents and what that will look like moving forward.
- Michigan has concerns due to our reporting timeframes as our statute requires that companies notify DIFS within 10 days of a cybersecurity incident that could affect Michigan residents. Could the IDSM Compliance Guide provide some guidance regarding referencing individual state notification requirements?
- DIFS Market Regulation currently does not upload cybersecurity investigations into NAIC systems; however, entering cybersecurity investigations into MATS has been considered.
- DIFS has concerns regarding the relevancy of utilizing IT financial exams that were in some cases completed three years prior to the current breach being reported.

    - This may place an additional burden on the companies to explain what material changes have been made to their IT systems over a lengthier period than cybersecurity investigations are presently considering.
    - In Michigan, this new process will broaden the responsibility for the IT financial exams team as they are not currently involved in investigating cybersecurity breaches.
- Will domestic regulators now be responsible for ensuring that all consumers are notified, including those in foreign jurisdictions?
- At the NAIC Summer National Meeting, it was mentioned that the cybersecurity repository is still being developed; DIFS proposes that the cybersecurity repository be contemplated in the IDSM Compliance Guide.
- Given that the statutes and the requirements for attestations could vary by state, contacting the domestic regulator to ensure that a company has complied with their obligations may not necessarily ensure that the company is compliant with the foreign regulator's requirements.
    - Section 4(I) only certifies that a company be in compliance with the IDSM, it doesn't contemplate the cause of the breach and whether measures have been put in place to decrease the likelihood of a similar event.
    - Not all licensees submit the annual certification, only domestic insurers. (For example, producers, insurance agencies, TPAs, etc.) Not all licensees are equally required to notify or provide information across states; in addition, not all licensees may be subject to financial examinations.
        - What is the proposed process where licensees are not subject to IT financial examinations?

Decision Tree

- Michigan concurs with Dave Buono's (PA) suggestion that the working group first consider building into the framework questions about the impact on consumers in instances where company operations are impacted. This line of questioning would assist in determining if questioning should be delayed until the company can resume normal operations.

Sincerely,

Danielle M. Flores

Company Market Regulation Administrative Manager
Michigan Department of Insurance and Financial Services

ACLI
Financial Security for Life

September 15, 2025

Chair Michael Peterson
Cybersecurity (H) Working Group
NAIC
1100 Walnut Street, Suite 1000
Kansas City, MO 64106-2197

via Koty Henry at khenry@naic.org

Dear Chair Peterson:

Thank you for the opportunity to provide further comments on the Insurance Data Security Model Compliance Guide and Chief Financial Regulator Forum Referral Response exposures to the Cybersecurity (H) Working Group. We appreciated the incorporation of our previous combined comments with joint trades APCIA and NAMIC in August. After further review, we have the following brief comments and questions on the exposures. Overall, we appreciate the emphasis on reducing duplicative oversight and support the emphasis on gap analysis as a tool to align IT reviews with Model 668.

- State-to-State Communication: We support the language in the CFRF Response noting the importance of communication among states to reduce duplicative efforts. Along those lines, would there be any guidance on how to facilitate information sharing if another state requests that information? Explicit guidance or suggested documentation might better facilitate this type of information-sharing practice between states.

- Market Conduct Coordination: We support the alignment of market conduct coordinated examinations and appreciate the effort to provide consistency in this area. There are currently issues with keeping information current during an exam as well as expertise of the examiner. This issue could be improved by creating NAIC-based examiner training and potentially aligning training guidance on interpretation of NIST 2.0 aligned controls in the context of Model 668. Examiner training could also leverage existing IT reviews during both financial and market conduct examinations. Because of the complex nature of the information within exams, if a licensee has a review by an outside third party which aligns with the requirements documented here, would licensees also be able to utilize this work as sufficient for a state? This would also aid in improved examinations and reduced duplication.

- **Multi-State Submission and Confidentiality:** In order to support further coordination, would the NAIC Cybersecurity portal support consolidated submissions for multi-state incidents tied to multiple entities? How would confidentiality be maintained across departments?

- **Incident Response and Event Reporting:** The inclusion of cybersecurity governance and breach notification prompts via pre- and post-incident checklists is a strong concept and we recommend alignment of those checklists with Model 668 as well as, where possible, NIST 2.0 to ensure consistency in expectations and reporting.

- **Regulatory Submissions to the NAIC:** What legal safeguards are currently in place to ensure proprietary or sensitive information provided by insurers or consultants is protected under applicable FOIP statutes? More specifically, how would you reconcile disclosure obligations under subpoena with the confidentiality protections afforded by individual state laws, namely where certain jurisdictions explicitly prohibit the release of such information even under judicial compulsion?

Once again we appreciate the effort to harmonize and improve upon the Compliance Guidance document and can provide any necessary follow-up. Please let us know if you have any questions.

Thank you,

Kirsten Wolfford
Senior Counsel, Privacy and Cybersecurity
ACLI
(202) 624-2059
kirstenwolfford@acli.com

September 15, 2025

Michael Peterson, Chair
Cybersecurity (H) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

By Email to: Koty Henry at KHenry@NAIC.org.

Re: NAIC Cybersecurity (H) Working Group Chief Financial Regulator Forum (CFRF) Referral Response and Insurance Data Security Model #668 (IDSM) Compliance Guide

Dear Mr. Peterson:

On behalf of AHIP, thank you for the opportunity to submit comments on the exposed CFRF Referral Response and IDSM Compliance Guide.

AHIP appreciates the NAIC's effort to promote consistent and effective cybersecurity oversight through the IDSM Compliance Guide. The guidance provides a good foundation for minimizing duplication through gap analysis and improving coordination across states. However, we continue to encourage on-going dialogue to ensure alignment with existing federal health care data security laws, particularly the Health Insurance Portability and Accountability Act (HIPAA). As you know, health insurers are already subject to comprehensive privacy, security and incident response requirements through the HIPAA Security Rule.

To enhance clarity, alignment, and ensure that IDSM implementation is consistent and coordinated with existing oversight, AHIP continues to encourage NAIC and this Working Group to continue to engage with health care stakeholders in the development of future resources for regulators.

For health insurance-specific guidance related to the IDSM, AHIP respectfully recommends the following issues be noted in the Compliance Guide for regulators' awareness and improved efficiency:

- **Safe Harbor for HIPAA-Covered Entities.** While state IDSM laws vary, recognizing HIPAA compliance is important as it simplifies the IDSM review process.

- **Acknowledgement of Existing Federal Oversight.** This will increase regulatory efficiency by avoiding duplicating efforts when federal oversight addresses similar controls.

- **HIPAA Crosswalk and Gap Analysis Tools**. AHIP continues to recommend the Working Group develop optional templates to help examiners align IDSM sections (such as the Cybersecurity Event Notification requirements of Section 6) with long-standing and proven HIPAA standards and requirements.

Thank you for the chance to comment. AHIP looks forward to further discussions with the Working Group.

Sincerely,

Miranda Motter
AHIP Senior Vice President, State Affairs and Policy
mmotter@ahip.org
202-923-7346

NAMIC
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

317.875.5250 | [F] 317.879.8408
3601 Vincennes Road, Indianapolis, Indiana 46268

202.628.1558 | [F] 202.628.1601
20 F Street N.W., Suite 510 | Washington, D.C. 20001

September 15, 2025

Michael Peterson (VA), Chair
NAIC Cybersecurity (H) Working Group
c/o Koty Henry, Cybersecurity Policy Advisor
Via email khenry@naic.org

Re: NAMIC Comments on the Cybersecurity (H) Working Group Insurance Data Security Model Law # 668 Compliance and Enforcement Guide

Dear Chair Peterson and Members of the Working Group:

On behalf of the National Association of Mutual Insurance Companies (NAMIC)[1], we would like to thank the NAIC Cybersecurity (H) Working Group for providing an extended review period and accepting additional comments on its Insurance Data Security Model Law # 668 Compliance and Enforcement Guide.

NAMIC previously submitted joint comments with the American Property Casualty Insurance Association (APCIA) and the American Council of Life Insurers (ACLI) on August 5, 2025, during the first round of requested feedback. NAMIC appreciates the Working Group incorporating a number of those suggestions in the recent exposure of the guide. One of the suggestions from our previous letter, however, does not appear to have been incorporated in the recent exposure – that being a clarification on when and why the guide should be used. While the Insurance Data Security Model Law # 668 is referenced throughout the compliance guide, there is no explicit instruction that the compliance guide itself and the flowchart apply only in instances where the examining state has adopted Model # 668. We also suggest that an explicit reference should be included as to how a review is triggered.

We therefore again raise our suggestion that the compliance guide clarify when and why the guide should be used. As stated in our joint trade letter dated August 5, 2025:

> The flowchart and compliance guide should clearly indicate that they apply only in instances where the examining state has adopted the NAIC Insurance Data Security Model Law (#668). Without this clarification, the guidance could be interpreted as encouraging non-adopting states to apply standards they have not formally enacted, potentially overstepping state authority. Clarifying this limitation would help preserve state autonomy while supporting consistent and appropriate implementation of the model where it has been adopted.

[1] The National Association of Mutual Insurance Companies consists of over 1,300 member companies, including six of the top 10 property/casualty insurers in the United States. The association supports local and regional mutual insurance companies on main streets across America as well as many of the country's largest national insurers. NAMIC member companies write $383 billion in annual premiums and represent 61 percent of homeowners, 48 percent of automobile, and 25 percent of the business insurance markets. Through its advocacy programs NAMIC promotes public policy solutions that benefit member companies and the policyholders they serve and fosters greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.

To avoid creating an unintended expectation that all states should conduct independent compliance assessments, we recommend the document explicitly state that this guidance is intended to support instances when a compliance review is appropriate. It should be made clear that such a review is generally triggered by (1) a financial examination conducted by the domestic state, (2) a market conduct examination, or (3) a specific infraction requiring investigation. While the guidance touches on this in various places, a more prominent explanation at the outset would help frame the appropriate use and scope of this tool. Likewise, we recommend revising the flowchart so that Step One includes identifying whether a regulatory trigger exists at all for a compliance inquiry.

We respectfully suggest that these clarifications have not been explicitly made and believe them to be important clarifications that the Working Gorup should incorporate into the flowchart and compliance guide.

In closing, NAMIC again thanks the Working Group for the extended review period and accepting additional comments, and for allowing engagement on the efforts to promote regulatory coordination and reduce unnecessary duplication in compliance assessments.

Sincerely,

Lindsey Klarkowski
Policy Vice President – Data Science, Artificial Intelligence, and Cybersecurity
NAMIC