2023 BOSTON

Navigating Data Privacy Infrastructure and Regulations

NCSHA
National Council *of* State Housing Agencies

Speakers

- **Discussion Leader**:
  Howard Tolley, Compliance Manager Utah Housing Corporation

- **Paul Hagerty**, IT Director | MassHousing
- **Cynthia Larose**, Member/Chair, Privacy and Cyber Security Practice | Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, PC
- **Angela Lee Chan**, Special Counsel – Information Officer | MassHousing

2023 BOSTON

Navigating Data Privacy Infrastructure and Regulations

Cynthia Larose

October 2023

NCSHA
National Council of State Housing Agencies

The "New" GLBA Safeguards Rule

- Applies to "financial institutions"
- Originally published in December 2021
- Rules (finally) became effective in June 2023
- Applies to all collection, storage, and use of "consumer" and "customer" personal information

So What Actually Is "New?"

- "Single Qualified Individual" to oversee the information security program
- Periodic risk assessments (at least annually)
- Use the risk assessment to implement appropriate security controls
- Regular testing
- Information security training
- Vendor risk management
- Incident response plan
- Annual reports to governing body

What is a Risk Assessment?

- Start by locating sensitive data – you can't protect it if you don't know where it is
- Develop a structured process against industry-standard frameworks (see 16 CFR 314.3 and 314.4) for Safeguard Rule stipulations
- Risk assessment is a team sport – it belongs to the enterprise and not "just IT"
- Looking for a place to start? The NIST Cybersecurity Framework contains a crosswalk to GLBA and the Safeguards Rule to help guide and explain

Vendor Oversight

- Important Safeguards Rule requirement
- Third party vendors post significant risk to nonpublic personal information and GLBA-covered entities are responsible for vendor oversight
- According to a recent study, 54% of organizations were breached through third parties in 2022
- Not all vendors present a material third party risk – look at your critical vendors who have access to customer NPI
- Minimum security requirements should be defined by contract and reviewed annually for compliance
- Request certifications, security assessment reports, penetration testing reports

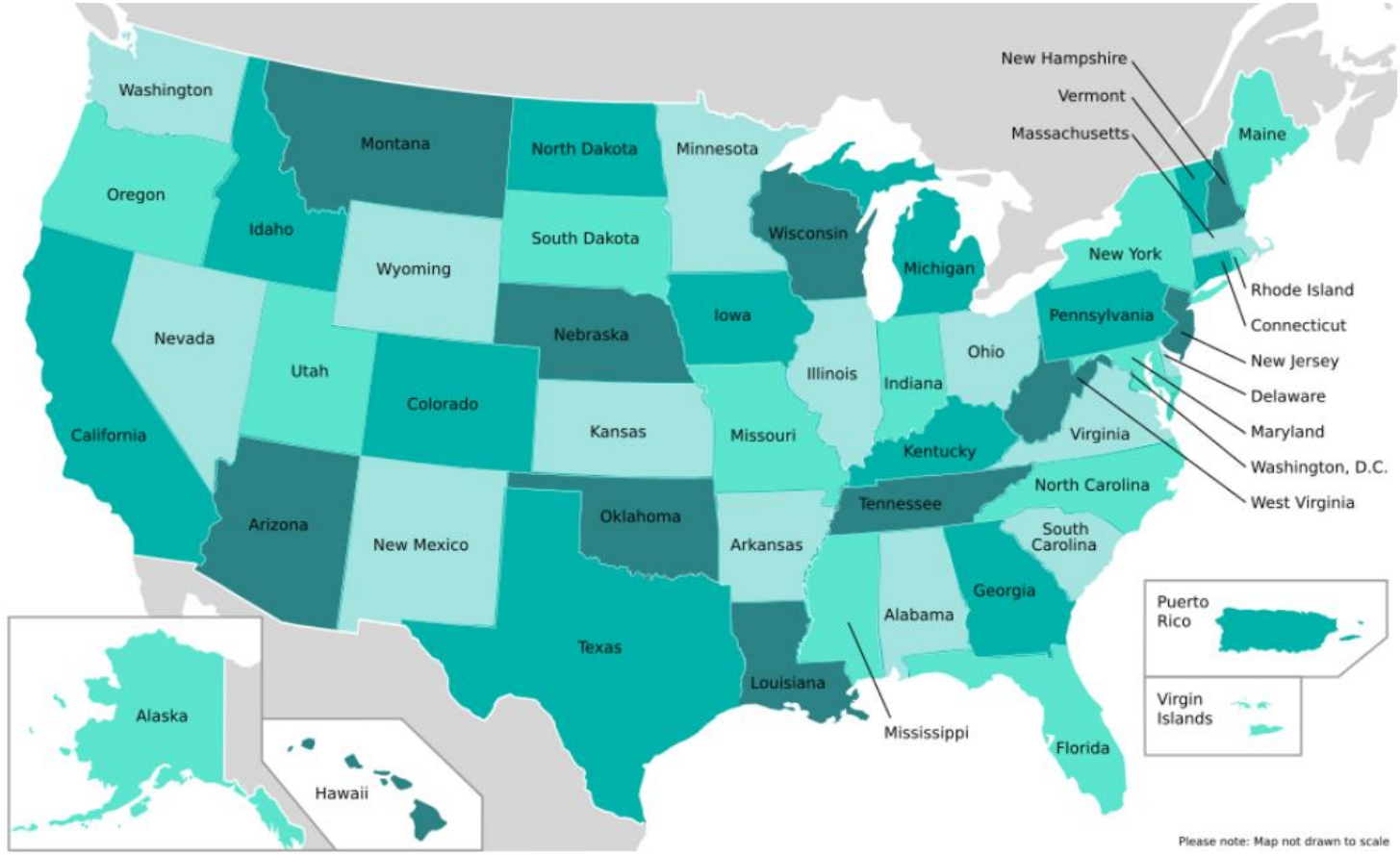
Vendor Oversight (continued)

- Use standard questionnaires
- Document risk analysis in a risk register – important tracking tool if something goes wrong
- Continuous monitoring
- You can outsource the function, but you cannot outsource the risk
- Plan for an incident – in the event of a data breach at a vendor, the data owner (read: your agency) has the ultimate responsibility for compliance with state data breach notification laws

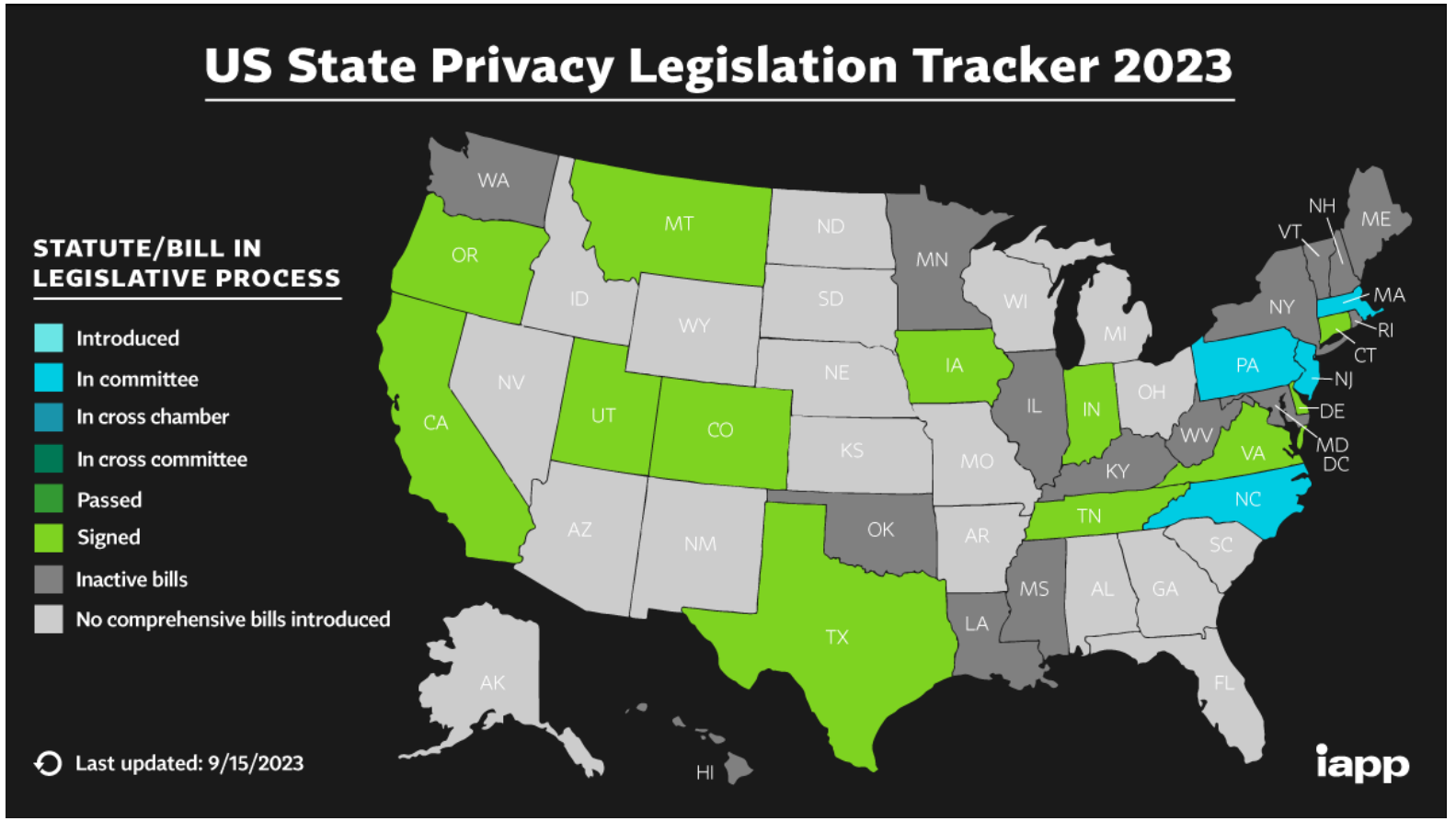
Speaking of State Data Breach Notification Laws

- Mintz Matrix

https://www.mintz.com/mintz-matrix



The US State Privacy Landscape: The Only Constant is Change



2023 BOSTON

THANK YOU

Cynthia Larose
CKLarose@mintz.com
617.348.1732

NCSHA
National Council of State Housing Agencies

2023 BOSTON

1. MassHousing's Information Security Mission and Infrastructure
2. Compliance - Managing Changing Data Privacy Regulations
3. Data Management RFP Lessons Learned

Navigating Data Privacy Infrastructure and Regulations

Angela Lee Chan | Special Counsel - Information Officer
Paul J. Hagerty | Director of Information Technology

NCSHA
National Council *of* State Housing Agencies

1 MassHousing's Information Security Mission and Infrastructure

Overview of Information Security Structure

- MassHousing's IT Cyber Security Team and the IT Security Committee **are led by IT**.
- Having **cross-departmental groups** working together helps further the information security mission.
- MassHousing is developing an additional Data Management Team.

A. Information Technology (IT) Security Committee

- Purpose | Driving cyber security efforts at MassHousing, including considering **IT infrastructure, network, assets, and data**. Preventing data breaches and monitoring and reacting to attacks.
- Departments Represented | IT, Homeownership, Rental, Finance, Internal Audit

B. Information Security Task Force

- Purpose | Recommend solutions related to **establishing and monitoring agency-wide information security policies, guidelines, standards**, and performing other duties as assigned. Identify and assess Agency information security, privacy and compliance needs and assists with their development and implementation.
- Departments Represented | Legal, Finance, Homeownership, Rental, Human Resources, IT

Legal Involvement

- The majority of attorneys focus on deal closings, so the *Special Counsel – Information Officer* role was created.
- The General Counsel recognized the **need to focus on MassHousing's data protection needs** and advocated for this unique role.

- In 2022, MassHousing's staff of 9 attorneys and 3 paralegals were focused on deal closings so were not involved in IT projects.
- The *Special Counsel - Information Officer* role was created in 2022 to work on **compliance and procurement activities** as well as to answer questions related to **ethics, public records, and records retention**.
- The Executive Director and General Counsel recognized the need to **fill the gap for other legal work at MassHousing unrelated to deal closings**.

2 Compliance – Managing Changing Data Privacy Regulations

Safeguards Rule

Lessons Learned:

1. Working inter-departmentally helps avoid unnecessary work.
2. Everyone brings their own expertise; rather than thinking about data as a strictly IT issue, **it's better to expand the groups working on it**.

- Context | The FTC required HFAs to **comply with the recently updated Safeguards Rule**, which requires financial institutions under FTC jurisdiction to have **measures in place to keep customer information secure**.
- Outcome | MassHousing would have gone down a rabbit hole figuring out new compliance measures, but Legal checked with outside counsel to learn that MassHousing was already in compliance by **having an ISP and being in compliance with M.G.L. c. 93H**.

Third-Party Risk Management

Lessons Learned:

1. Third-party vendor relationships are an Agency issue not just an IT issue.

2. Having staff members outside of IT who understand the importance and requirements of securing data can help IT identify potential gaps in their management of data.

- Context | In June 2023, the Federal Registrar released the Final Interagency Guidance for Third-Party Risk Management Programs offering **financial institutions more direction on how to improve risk management practices and the safeguarding of data**.
- Outcome | The reaction by MassHousing was similar to that of the Safeguards Rule. Legal again consulted outside counsel who confirmed that MassHousing's ISP already contained several requirements in the Guidance, but would need to include a few additional practices to meet the guidance.

3

Data Management
RFP Process
Lessons Learned

Data Management

- The project was sponsored by the Chief Financial & Administrative Officer, who has asked over several years for the Agency to undertake this initiative.

Context |

- Even with a robust Information Security Program (ISP) it is important to **know your data in order to protect it**.
- Data management is a challenge at any HFA given the amount of personal information (PI) we deal with.
- MassHousing sought to **better identify all data storage locations, maintain data security, classify structured and unstructured data, reduce wasteful data redundancy, ensure data integrity, and improve data accessibility**.

RFP 1 (Failed)

Lessons Learned:

1. Need to **break bigger projects into component parts**.
2. Do more research by **talking to experts or other agencies** to figure out first steps.

- RFP | MassHousing initially put out an RFP for "assistance with implementing a data management program to **analyze and clarify our structured and unstructured data**."
- The way we scoped the project proved to be **too much for one contract and too broad in scope.**
- Outcome | MassHousing received one response to the RFP, and after working together for under three (3) months, we realized we were spinning our wheels and ended the engagement.

RFP 2

- MassHousing worked with Microsoft to **outline our needs and narrow the scope** for the first part of the project.
- The revised RFP focused on **developing a data inventory** so MassHousing can understand its data.

- Revised RFP | MassHousing put out a more **limited Data Inventory RFP** as a first step with the goal to develop a **data inventory that will be a comprehensive catalog or map of its data assets**. The data inventory will be a **record of all data assets** organization-wide and include other details such as owner, name, source, format, access permissions and other properties.
- Goal | MassHousing is seeking to ensure that it **fully understands its data to derive valuable insights** including how data points interact with other data, how data flows, and how to protect data.

RFP 2 Progress to Date

Lessons Learned so far:

1. A **clear, manageable project scope** led to good RFP responses.
2. Leadership buy-in is fundamental.
3. Staff buy-in and involvement is also critical, rely on **leadership to help deliver the message and goals of the project**.

- MassHousing got **14 responses to RFP** and are currently engaged with a firm have that has experience and expertise in this area.
- We have been meeting since August and are making progress.
- Questionnaires have been sent to **88 staff member partners throughout the Agency to understand how data is being accessed**.
  - Buy-in from our partners and getting them to respond to the questionnaire has been mixed.
  - It is **important and helpful to get leadership involved to help deliver the message and goals of the project**.
  - Of the 88 data partners, there were 8 people (9%) who didn't respond after an email message from our Chief Financial & Administrative Officer.
- After an analysis and review of the response, the next step will be to analyze and conduct data partner interviews to validate MassHousing's data footprint, after which we will build a data inventory and gauge partners for feedback. We anticipate that this engagement will take until next spring to complete.

Lessons Learned

1. Don’t settle!
2. Be willing to move on.
3. Ask for help.
4. Try, try again… it’s too important.

2023 BOSTON

Questions?

NCSHA
National Council *of* State Housing Agencies