WEST VIRGINIA

STATE PRIVACY OFFICE

2020-21 Annual Report

FEBRUARY 2022

Ashley Summitt, Chief Privacy Officer
Lori Tarr, Assistant Chief Privacy Officer

Sue Haga, Administrative Assistant

Membership of the 2020-21 Privacy Management Team (PMT)

Board of Risk and Insurance Management, State Privacy Office (a unit of BRIM):

- BRIM – Mary Jane Pickens (Executive Director)
- BRIM – Robert Fisher (Deputy Director)
- State Privacy Office – Ashley Summitt (Chief Privacy Officer)
- State Privacy Office – Lori Tarr (Assistant Chief Privacy Officer)
- State Privacy Office – Sue Haga {2020} (Administrative Secretary), Tara Taylor {2021} (Administrative Assistant)

Executive Branch, Department Privacy Officers (DPO), Agency Privacy Officers (APO):

- Governor's Office – Berkeley Bentley {2020} (DPO), Garner Marks {2021} (DPO), Felicia Swecker (APO)
- Bureau of Senior Services – Lee Knabenshue (DPO)
- Department of Administration –Tom Miller (DPO HIPAA), Misty Peal (Non-HIPAA)
    - Secretary's Office – Misty Peal (DPO)
    - Cyber Security Office – Danielle Cox (Chief Information Security Officer)
    - Office of Technology –Jennelle Jones (General Counsel)
    - PEIA – Ted Cheatham (Director) {2020}, Jason Haught (Interim Director) {2021}
    - PEIA – Tom Miller (HIPAA Privacy Officer) and Bill Hicks (General Counsel)
    - Division of Personnel – Wendy Mays (APO)
- Department of Arts, Culture and History – Kristopher Bowyer (DPO)
- Department of Commerce – Steve Meester (DPO)
    - Workforce WV – Jonathan Link {2020}(APO), David Dyer {2021} (APO)
    - Division of Rehabilitation Services – Brenda Bates{(2020} (APO), Aaron Johnson {2021}
- Department of Environmental Protection – Neil Chakrabarty
- Department of Economic Development - Steve Meester (DPO)
- Department of Health and Human Resources – Chris Snyder (DPO),
    - Represents Bureau of Public Health–Claire Winterholler (Assistant Attorney General)
- Department of Homeland Security– Jamie Chambers (DPO)
- Department of Revenue – Allen Prunty (DPO)
- Department of Tourism - Erica Whitney (DPO)
- Department of Transportation – Jill Dunn (DPO)
    - Division of Highways – Jennifer Pierson & Jennifer Rutherford (APOs)
    - Division of Motor Vehicles – Rebecca McDonald {2019}, Jennifer Pierson {2020}
- Department of Veterans Assistance –Maria Yoakum {2020} (DPO), Julie Reed {2021} (DPO)
- Chapter 30 Licensing Boards –Sue Painter (Privacy Liaison)
- West Virginia National Guard - Mountaineer Academy North - Deborah Gipson, (APO)
- West Virginia National Guard - Mountaineer Academy South -

Representing Other Constitutional Officers and Higher Education:

- State Auditor's Office – Michael Nusbaum
- Department of Education – Georgia Hughes-Webb
- State Treasurer's Office – Brian Bailey, Lisa Rutherford

- West Virginia Supreme Court of Appeals - Pat Moats
- West Virginia School of Osteopathic Medicine – Jeffrey Shawver, Deborah Bogan
- West Virginia University – Alex Jalso (Chief Information Security and Privacy Officer){2020}, Amanda Griffith {2021}
- West Virginia University – Sandy Price (Health Sciences Center Risk Mgr. / Privacy Officer)
- West Virginia Higher Education Policy Commission/West Virginia Community and Technical College System – Pam Woods {2020}, Melanie Baker {2021}, Shelley DeLuca {2021}, Zorrie Georgieva {2021}
- Marshall Health – Buffy Hammers
- wvOASIS – Richard Dolin

INTRODUCTION

Under the direction of the Executive Director of the Board of Risk and Insurance Management (BRIM), the State Privacy Office (SPO) manages the executive branch's Privacy Program (Program) and leads the Privacy Management Team (PMT). The SPO consists of the Chief Privacy Officer (CPO), the Assistant Chief Privacy Officer (ACPO), and an Administrative Assistant.

The PMT consists of:

- leadership at BRIM;
- the State Privacy Office;
- privacy officers from each department and many agencies, higher education, other state constitutional officers, and other branches of state government; and
- the Chief Information Security Officer (CISO).

The SPO and the PMT efforts may be described in three broad functions: accountability; risk management; and, compliance. The goal is to protect the personally identifiable information (PII) of the state's citizens and workforce. PII includes other subcategories of information such as Protected Health Information (PHI), Federal Tax Information (FTI), and Payment Card Industry (PCI) information.

Six Guiding Principles for the State Privacy Program

These six guiding principles are foundational to any privacy program and are used as the basis for the West Virginia Executive Branch Privacy Policies and guide the State Privacy Office in all aspects of our program.

- *Accountability* – assigned roles and responsibilities to assure application of privacy principles to PII.
- *Notice* – openness regarding the authority for collecting PII; the purpose of the collection; the location of the entity maintaining the PII; with whom the PII may be shared and why; rights an individual has in PII; and the entity's policies, procedures, standards, and practices with regard to PII.
- *Minimum Necessary and Limited Use* – collection, use and disclosure of PII should be limited to the entity's legal authority and purpose, as set forth in an entity's Notice, and Minimum Necessary PII the entity needs to perform the defined legally permitted task.

- *Consent and Authorization* – an entity's collection of PII should be contingent upon first obtaining an individual's consent to collection. An entity does not collect, use, or disclose PII in a manner inconsistent with its Notice, unless it has first obtained the individual's permission for the use or disclosure.
- *Individual Rights/Individual Participation* – when possible, an entity relies first on the PII it collects directly from the individual. An individual should be afforded the ability to access and copy the PII an entity acquired or maintains, request an amendment of the information an entity maintains and, if such amendment is not undertaken, request that the information be notated. Entities shall provide appropriate means of individual redress which include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed.
- *Security Safeguards* – an entity implements the appropriate management, operational and technical controls to preserve the privacy, confidentiality, integrity and availability of PII.

ACCOUNTABILITY

State leadership is committed to proactive accountable management of information security and privacy. The foundational policy of the Privacy Program is the Accountability Policy. This requires each department to have one or more privacy officers designated to ensure application of the executive branch privacy policies and procedures, and to provide training to the departments' workforce. Having staff dedicated to the task of data privacy is intrinsic to holding ourselves accountable to our citizens and workforce.

Fundamental to the process of preparing new privacy officers, is our office's privacy officer orientation process. This training reviews the organization of the Privacy Program, the important role it plays in the protection of the state's data, privacy policies, and incident management. It also reviews the privacy impact assessment, online privacy training of the workforce, privacy resources, and many other aspects of the privacy officer role.

The number of new privacy officer orientations conducted in 2020 and 2021 were 3 and 10, respectively. This was a significant reduction from 2019, when there were 20 orientations. With retirements and the Privacy Office's efforts to secure privacy officers for previously non-represented agencies, we anticipate 2022 will be back at 2019 orientation levels. Typically, department privacy officers train agency privacy officers, but with the large number of new department and agency privacy officers, providing the training in-house, was a prudent and effective step.

The commitment to privacy by West Virginia's leadership is underscored by an annual proclamation of Data Privacy Day, which is an internationally recognized day each January 28. The proclamation encourages observance of Data Privacy Day by government officials and representatives, educators, schools, and citizens. Each year the SPO holds a West Virginia Data Privacy Day event to raise awareness and provide additional training to all executive branch

departmental privacy officers. The training activities for the 2020 Data Privacy Day event were held in person and were led by the state's breach coach, who is an attorney and a cybersecurity expert. The topic was Payment Card Information (PCI) and included members of the West Virginia Treasurer's Office due to its role in providing the e-Government Services Program, which includes efforts to secure PCI data. Fifty-five members of the Privacy Management Team and the Treasurer's Office attended the event.

The 2021 Data Privacy Day was conducted virtually due to the Covid pandemic. Because of the use of the virtual format, the event was opened to both departmental and agency privacy officers alike as a means to provide a training benefit to agency privacy officers. The 2021 Data Privacy Day event was a panel discussion of a holistic approach to cybersecurity and was led by the state's breach coach, and cybersecurity experts from the cyber insurance market.

In addition to its focus on the future and advancing the Privacy Program, the SPO also continued to promote accountability and fulfill its management role by:

- Leading the quarterly PMT meetings, which provide a forum for training and information sharing, legislative updates, consensus building, security updates, and open dialogue among PMT members. The SPO sets the agendas for each meeting, providing speakers and experts in the relevant fields. Since the format of the PMT has been virtual meetings since the pandemic began, PMT meetings have included more agency privacy officers.

- In 2020, discussions and training were based on current privacy and security issues and on members' requests and included:

    - NIST Privacy Framework
    - Incident Management Case Studies
    - Risk Assessment
    - Public Health and Privacy
    - HIPAA Preemption Analysis and Privacy Legal Update

- In 2021, the topics presented and discussed at the PMT included:
    - Incident Management Case Studies
    - HIPAA Updates - Office of Civil Rights Presentation
    - Artificial Intelligence
    - Risk Assessment
    - HIPAA Preemption Analysis and Privacy Legal Update.

Risk Management

Mitigating organizational risk is accomplished through the selection of appropriate privacy controls established through organization-wide assessment and understanding of distinct mission/business and operational needs. According to the National Institute of Standards and

Technology, "The risk-based approach…considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, or regulations."[1]

Activities by the SPO supporting and enhancing risk management included:

- Review of PIA submissions. The PIA provides project managers with a risk assessment tool for reviewing privacy implications involved with the purchase of information technologies or system redesign processes that collect or store PII. The PIA includes: a privacy threshold analysis; a review of data classification and collection, use and storage factors; disclosure practices; and administrative, physical and technical controls.

  Submissions of PIAs increased approximately twofold in 2020 and 2021
  - 2019 – 25
  - 2020 – 48
  - 2021 – 52

- Regular collaboration between the CPO and the CISO regarding risk management, incident response, strategic planning, and workforce development.

- Participation by the SPO with the CISO in a Risk Assessment RFP. WV Board of Risk and Insurance Management, of which the State Privacy Office is a division, took part in the Risk Assessment pilot as an initial agency.

- Training and education of the workforce continued to be a high priority for the SPO.

  According to the Ponemon Institute's 2020 Cost of Data Breach Study, training was one of the most effective factors for reducing the cost of a data breach. Twenty-five factors were reviewed in the study. Having an incident response team and use of incident response testing were other top factors. [2]

  Beyond the training completed for privacy officers or the regular PMT meetings, the following training was provided in 2020 and 2021:

  - January 2020 and 2021: Data Privacy Days, which included Payment Card Information substance, incident response workshops with table-top exercises involving ransomware and phishing, particular to PCI and an expert panel to discuss a holistic view of cybersecurity.
  - May 2020, SPO staff provided an online recorded webinar (Purchasing as a Privacy Powerhouse) for the Division of Purchasing's 2020 In-House Training Program.

[1] Dept. of Commerce. NIST. "Risk Management." Updated November 30, 2017. Accessed December 29, 2017. https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview.

[2] Ponemon Institute. "Cost of Data Breach Study: 2020." IBM Security. https://www.ibm.com/security/data-breach

- July 2020, SPO staff did a live virtual presentation for the West Virginia Department of Education in their annual training for County Board of Education Treasurers, entitled “Brim and Cyber Liability and Awareness.”
- August 2021, SPO staff presented virtually a privacy webinar entitled “Purchasing as a Privacy Powerhouse,” for the annual WV Purchasing Division Conference.
- September 2021, SPO staff presented to the Association of Governmental Accountants (AGA) a presentation entitled “West Virginia Privacy Program”.
- December 2021, the CPO presented the history of West Virginia’s cyber insurance coverage to a group of governmental Chief Privacy Officers at the NASCIO (National Association of State Chief Information Officers) conference.

- The SPO has been working with the other divisions within BRIM and within the Department of Administration to update their agency’s records retention and disposal schedule. Using the Retention schedule, many old files are being cleared out of their office and Iron Mountain (the state’s archive service) to be destroyed. Current files and documents are being scanned and retained electronically. These electronic documents are now considered the official documents of record. The electronic files will be purged as their disposal dates are reached. This is a risk management project that reflects the Minimum Necessary and Limited Use privacy policy by adhering to best practices for the data lifecycle of PII, which includes data destruction.

COMPLIANCE

The commitment to comply with internal policies, industry standards, and external regulations was demonstrated by the SPO with the following activities and projects:

- The SPO has provided assistance throughout the Covid-19 pandemic in reviewing privacy compliance issues. One such effort was working with the Department of Health and Human Services, and the Division of Personnel to review internal policies and regulations so that a COVID-19 Privacy Guidance could be issued at the outset of the pandemic.

- Management of the executive branch privacy incident response program to assure notification compliance with privacy laws. The SPO provides oversight and serves as a resource, throughout the duration of managing a privacy incident, from filing the initial report, through the investigation, to resolution. Due to an increase in numbers and complexities of incidents in 2019, the State Privacy Office is investigating an online incident management option.

- Oversight, tracking and reporting of required online privacy training courses for the state’s workforce, completed through the Learning Management System (LMS). These include the West Virginia Executive Branch Confidentiality Agreement, Privacy Awareness , and HIPAA/HITECH Awareness Training. The State Privacy Office contracted

with a privacy training provider to provide an updated general privacy training to be available on the LMS.

- Provided advice and consultation, as needed, to the state's workforce on privacy issues related to:
    - Executive branch contracts with vendors;
    - Privacy policies, procedures, laws, and regulations;
    - Incident investigation; and
    - Best practices in project design and implementation.

- Revised the annual Privacy Requirements Report. This is a review of new federal and state privacy laws that affect the executive branch. Each law is identified by common name, legal citation and description, implications, electronic source, and mapped to applicable privacy principles.

- Updated the annual HIPAA Preemption Analysis, which is an overview of the preemption issues that arise between state and federal law. The Privacy, Security, Breach Notification, and Enforcement Rules of HIPAA and the HITECH Act, and the requirements of West Virginia laws are compared to determine which laws are more stringent, and thereby supersede or preempt the other, to become the primary law for a particular aspect of health care privacy.

CONCLUSION

The SPO continues to work diligently to advance methods of operating a vibrant statewide privacy program with a very small staff. Being able to incorporate privacy technology into our means of operation is imperative to continue to mature our privacy program capable of proactively addressing the complexity of cybersecurity incidents that are occuring in our nation. Our commitment to protecting the privacy of the state's citizens and workforce remains high. We have had unexpected global challenges to address, but these are being overcome with necessary flexibility, ingenuity and dedication. We look forward to sharing in future reports the SPO's progress to grow and mature West Virginia's Privacy Program.

References

Dept. of Commerce. NIST. “Risk Management.” Updated December 13, 2017. Accessed December 29, 2017. https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview.

Ponemon Institute. “Cost of Data Breach Study: 2020.” IBM Security. https://www.ibm.com/security/data-breach