WEST VIRGINIA
STATE PRIVACY OFFICE

2018-19 Annual Report

SEPTEMBER 30, 2020

Ashley Summitt, Chief Privacy Officer
Lori Tarr, Assistant Chief Privacy Officer
Sue Haga, Administrative Secretary

Membership of the 2018-2020 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 – Sallie Milam {2018}, Ashley Summitt {2019} (Chief Privacy Officer)
- State Privacy Office – Lori Tarr (Assistant Chief Privacy Officer)
- State Privacy Office – Sue Haga (Administrative Secretary)

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

- Governor's Office – Ashley Summitt (DPO) {2018}, Berkley Bentley {2019}
- Bureau of Senior Services – Lee Knabenshue (DPO)
- Department of Administration –Tom Miller (DPOHIPAA), Misty Peal (Non-HIPAA) {2019}
    - Secretary's Office – Jennelle Jones (Deputy General Counsel) {2018}, Misty Peal {2019}
    - Cyber Security Office – Danielle Cox (Chief Information Security Officer) {2019}
    - Office of Technology – Josh Spence (Chief Information Officer) {2018}, Jennelle Jones (General Counsel) {2019}
    - PEIA – Ted Cheatham (Director)
    - PEIA – Tom Miller (HIPAA Privacy Officer) and Bill Hicks (General Counsel)
    - Division of Personnel – Wendy Elswick (APO)
- Department of Arts, Culture and History – Kristopher Bowyer (DPO)
- Department of Commerce – Debe Browning (DPO)
    - Workforce WV – Angie Richardson (APO)
    - Division of Rehabilitation Services – Brenda Bates (APO)
- Department of Environmental Protection – Lori Saylor {2018}, Neil Chakrabarty {2019}
- Department of Health and Human Resources – Chris Snyder (DPO),
    - Represents Bureau of Public Health–Claire Winterholler (Assistant Attorney General)
- Department of Military Affairs and Public Safety – Bryan Arthur
- Department of Revenue – Misty Peal (DPO) {2018}, Allen Prunty (DPO) {2019}
- Department of Transportation – Karen Saunders (DPO) {2018}, Jill Dunn (DPO) {2019}
    - Division of Highways – Karen Saunders {2018} Jennifer Pierson & Jennifer Rutherford (APOs) 2019
    - Division of Motor Vehicles – Joyce Abbott (APO) {2018}, Rebecca McDonald {2019}
- Department of Veterans Assistance – Ron Mooney (DPO)
- Chapter 30 Licensing Boards –Sue Painter (Privacy Liaison)

Representing Other Constitutional Officers and Higher Education:

- State Auditor's Office – Michael Nusbaum
- Department of Education – Georgia Hughes-Webb
- State Treasurer's Office – Kin Richardson, Lisa Rutherford
- West Virginia School of Osteopathic Medicine – Jeffrey Shawver, Deborah Bogan
- West Virginia University – Alex Jalso (Chief Information Security and Privacy Officer)
- 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
- Marshall Health – Buffy Hammers, Cindy Shrout
- wvOASIS – Richard Dolin

STATE OF WEST VIRGINIA
DEPARTMENT OF ADMINISTRATION
BOARD OF RISK AND INSURANCE MANAGEMENT

Allan L. McVey
Cabinet Secretary

Mary Jane Pickens
Executive Director
Deputy Cabinet Secretary

September 30, 2020

Mr. Mike Hall, Chief of Staff
Office of the Governor
State Capitol
1900 Kanawha Blvd. E
Charleston, WV 25305

Dear Mr. Hall:

I am pleased to submit to Governor Justice and to you the Board of Risk and Insurance Management's annual report on West Virginia's privacy program. This is the first report after the successful transition to a new Chief Privacy Officer (CPO) at the State Privacy Office (SPO) in 2019. This change, along with the turnover of multiple privacy officers throughout the executive branch, necessitated a delay in issuing the report; and a decision was made to cover both 2018 and 2019 in one report. The report also is divided into three sections covering accountability, risk management, and compliance.

The vision formed from the SPO's strategic plan for 2018 – 2020 was reaffirmed during this period of significant change. The need to transition from the present labor-intensive method for incident management to a technology-based approach is even more clear with the turnover that occurred in the program of experienced privacy officers. Therefore, BRIM and the SPO will be re-doubling efforts, working with WV Office of Technology, to purchase and establish privacy technology solutions that will be effective and efficient. Through accountability measures, privacy risk management and legal compliance, we continue to mature the state's privacy program.

Maintaining our citizens' and employees' privacy is a priority for all of us at the Board of Risk and Insurance Management and the State Privacy Office. This requires a variety of ongoing proactive efforts, along with focused management of privacy incidents to protect the state's valuable data assets, which is our ultimate goal. Thank you for your continued support toward this mutual effort

Should you have any questions, please contact Chief Privacy Officer Ashley Summitt at 304-766-2646 X 20232.

Very truly yours,

Mary Jane Pickens
Executive Director

MJP/ldm
Enclosure

1124 Smith Street, Suite 4300
Charleston, West Virginia 25301
www.brim.wv.gov

(304) 766-2646
(304) 558-6004 FAX
(800) 345-4669 TOLL FREE WV

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 Secretary.

The PMT consists of:

- leadership at BRIM;
- the State Privacy Office;
- privacy officers from each department and many agencies, higher education, and other state constitutional officers; 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.

ACCOUNTABILITY

State leadership is committed to proactive accountable management of information 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.

With the close of 2018, and throughout 2019, the efforts of the SPO were focused, out of necessity, on staffing. In December 2018, Sallie Milam, the state's first CPO who helped establish the Privacy Program, retired from state government to take a position in the private sector. Also, multiple departments within the executive branch experienced a change in appointed privacy officers.

In April 2019, we were pleased to have Ashley Summit, J. D., join BRIM and the SPO as the Program's new CPO. She was deputy general counsel and privacy officer for the Governor's

Office prior to joining the SPO. 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.

With the high degree of turnover experienced in 2019, our office provided an increased number of training sessions with not only new department privacy officers, but also agency-level privacy officers. In 2017, the Privacy Office provided 8 orientations, but in 2018 and 2019, the number of orientations that were provided by the State Privacy Office for new departmental and agency privacy officers more than doubled, with 18 sessions in 2018 and 20 in 2019. 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. Training content was also revised and advanced for the privacy officer orientations.

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 2018 and 2019 Data Privacy Days were led by the state's breach coach, who is an attorney and cybersecurity expert. These events included presentations on the current threat environment, ransomware, and phishing attempts as well as table-top exercises, which led participants to review steps to take with various scenarios, comparing these with our policies and procedures.

In 2018 the SPO worked with WV Interactive to redesign its website to match the design of the BRIM website. The privacy.wv.gov website is a repository of information on policies; legal analyses regarding state and federal laws and the intersection of FOIA requests and privacy; resources for incident response and privacy impact assessments; and, consumer links for information on identity theft and how to file a privacy complaint.

In 2017 the SPO adopted the American Institute of CPAs' (AICPA) Privacy Maturity Model, an internationally recognized framework for assessing strengths and weaknesses of a privacy program.[1] And, using this model, nine criteria were evaluated that fall under the privacy domain for advancing a privacy program:

[1] American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA). "Privacy Maturity Model." March 2011. https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf

1) Contracts with Clients, Partners
2) Infrastructure & Systems Management
3) Policy Documentation
4) Privacy Awareness & Training
5) Privacy Budget
6) Privacy Function
7) Privacy Incident Management
8) Privacy Personnel
9) Risk Assessment

Based on the criteria above, and completed with input from the PMT, the SPO has a three-year strategic plan. It has six objectives and addresses five of the nine AICPA criteria:

1. Increase the use of Privacy Impact Assessments (PIA). These assessments are used to evaluate the privacy implications of new technologies and systems that handle or collect PII. The PIA process is a recognized best practice used within the federal government and industry alike as a pro-active tool to build privacy into information systems. Since passage of the E-Government Act of 2002, PIAs have grown in usage in federal and state governments. In the passage of the Secure West Virginia Act of 2019, the PIA was defined in Code for further development and use within state government.

   The West Virginia Privacy Office is working collaboratively, with the CISO and the Vendor Management Workgroup, to establish protocols within the Purchasing and the Office of Technology Divisions to effectively implement a vigorous PIA process.

2. Implement a Privacy by Design (PbD) program, which is an approach that takes privacy into account throughout the entire development of information systems.[2]

   In 2018 the State Privacy Office held a two-and-half day privacy retreat at Canaan Valley State Park, which was focused on a better understanding of the concepts of PbD, and how our PIA procedure supports the PbD concept. This was presented by Bob Siegel, a Fellow in Information Privacy and founder of Privacy Ref, a privacy consulting firm. Attendees included privacy officers, and staff in the Cybersecurity Office and Purchasing Division. A table-top exercise was provided by our state's breach coach demonstrating the risk from a vendor with an unsecured cloud storage service and the importance of diligence up front.

3. Build an automated Incident Management System. This will be used to reduce risk, simplify compliance with data breach laws and expedite the process, which will free-up labor resources.

[2] Cavoukian, Ann. "Privacy by Design the 7 Foundational Principles." https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

The Office has begun discussions with vendors and consultants to learn about the options available for automated incident reporting and management solutions.

4. Implement a vendor management program, which will address risk assessments, privacy and security contract terms, and assurance.

   A Vendor Management Group was formed comprised of staff from the State Privacy Office, the Purchasing Division, the Office of Technology Division, and BRIM, to address these issues, including updating important privacy procurement forms and procedures.

5. Update and revise executive branch privacy policies and audit a representative sampling of agency privacy notices.

   Throughout our 2019 PMT meetings we reviewed each of the policies and received feedback from the departmental privacy officers for upcoming revisions to the policies.

6. Update HIPAA awareness training, which is a regulatory requirement and a proven risk reduction tool.

   The SPO initiated a process to procure updated HIPAA training that will be available to all staff of HIPAA impacted state agencies.

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 bi-monthly 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.

- In 2018, discussions and training were based on current privacy and security issues and on members' requests and included:

  - Vendor Assurance and Purchasing
  - Incident Response and Management (a year-long series)
  - GDPR Big Data and the Internet Payment Card Industry Awareness
  - Record Retention and Disposal Cybersecurity and Cyber Risk Management
  - Office of Civil Rights Increased Penalties
  - NIST Security Framework

- In 2019, the topics presented and discussed at the PMT included:
  - Secure West Virginia Act passage
  - WV CISO increased duties and authority
  - PCI DSS continuing discussion

- Privacy in Procurement and Contracting
- Minimum Necessary Principle in Procurement
- Advocating for a broader agency participation, both in and beyond the executive branch, in the PMT and in privacy trainings.

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."[3]

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 150% in 2019:
  - 2017 – 13
  - 2018 – 10
  - 2019 – 25

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

- Participation in a vendor management workgroup, which is identifying and resolving privacy and security risks associated with state services supplied by contract vendors. The workgroup began in September 2017 and is anticipated to continue indefinitely to address the changing risks faced in vendor management. The workgroup has identified three goals:

  - Empower agencies to accurately determine the level of risk associated with procurement of goods or services.

  - Review and develop appropriate privacy, security, and risk management contract terms and conditions.

[3] 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.

- Develop vendor assurance program which strategically monitors vendors' risk.

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

  According to the Ponemon Institute's 2019 Cost of Data Breach Study, training was one of the most effective factors for reducing the cost of a data breach. Twenty factors were reviewed in the study. Having an incident response team and extensive use of encryption were other top factors.[4]

  Beyond the training completed for privacy officers or the regular PMT meetings, the following training was provided in 2018 and 2019:

  - January 2018 and 2019: Data Privacy Days, which included incident response workshops with table-top exercises involving ransomware and phishing.
  - May 2018: BRIM Cyber Liability and Awareness - West Virginia Association of School Business Officials Spring Conference
  - May 2019: Purchasing as a Privacy Powerhouse – an in-house webinar for the Purchasing Division.
  - June 2018: Purchasing as a Privacy Powerhouse – an in-house webinar for the Purchasing Division.
  - August 2018: WV Privacy Retreat, which included a keynote address on HIPAA; presentations on Privacy Impact Assessments, Privacy-by-Design; and, table-top exercises.
  - September 2019: Privacy and Cybersecurity: A Partnership with Purchasing – presentation at the annual Purchasing Conference.
  - October 2018: Privacy and Cybersecurity: A Partnership with Purchasing – presentation at the annual Purchasing Conference.
  - October 2018: Privacy and Cyber Security Awareness - WV Real Estate Appraiser Licensing and Certification Board

- The SPO has been working with the other departments within BRIM to update the BRIM Records Retention and Disposal Schedule. Using the Retention schedule, many old files are being cleared out of the 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.

[4] Ponemon Institute. "2019 Cost of Data Breach Study: Global Overview." July 2019. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.130415692.259281279.1588011789-587497001.1588011789&_gac=1.259989112

COMPLIANCE

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

- 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 trainings for the state's workforce completed through the Learning Management System (LMS). These include the West Virginia Executive Branch Confidentiality Agreement, Think WV Privacy, and HIPAA/HITECH Awareness Training.

- 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 the projects and plans laid out in the 2017 strategic plan. Our commitment to protecting the privacy of the state's citizens and workforce remains high. We have had unexpected challenges since 2017 to address, but these are being overcome with necessary flexibility and dedication. We look forward to sharing in future reports the SPO's progress to grow and mature West Virginia's Privacy Program.

REFERENCES

American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA). "Privacy Maturity Model." March 2011. https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf

Cavoukian, Ann. "Privacy by Design the 7 Foundational Principles." https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

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, & IBM Security (2019). "Cost of a Data Breach Report 2019." June 2017. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.130415692.259281279.1588011789-587497001.1588011789&_gac=1.259989112