WEST VIRGINIA
STATE PRIVACY OFFICE

2017 Annual Report

DECEMBER 31, 2017

Sallie Milam, Chief Privacy Officer
Lori Tarr, Assistant Chief Privacy Officer
Sue Haga, Administrative Secretary

Membership of the 2017 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 (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)
- Bureau of Senior Services – Lee Rodgers (DPO)
- Department of Administration – Tom Miller (DPO)
  - Secretary's Office – Jennelle Jones (Deputy General Counsel)
  - Cyber Security Office – Josh Spence (Chief Information Security Officer)
  - Cyber Security Office – Danielle Cox (Cybersecurity Administrative Manager)
  - PEIA – Ted Cheatham (Director)
  - PEIA – Bill Hicks (General Counsel)
  - Division of Personnel – Wendy Elswick (APO)
- Department of Commerce – Debe Browning (DPO)
  - Workforce WV – Angie Richardson (APO)
- Department of Education and the Arts – Brenda Bates (DPO)
- Department of Environmental Protection – Lori Saylor (DPO)
- Department of Health and Human Resources – Lindsey McIntosh (DPO),
  - Bureau of Behavioral Health and Health Facilities – Gail Noullet (APO)
  - Represents Bureau of Public Health–Claire Winterholler (Assistant Attorney General)
  - West Virginia Health Information Network – Denise Hershey (APO)
- Department of Military Affairs and Public Safety – Rick Staton (DPO)
- Department of Revenue – Misty Peal (DPO)
- Department of Transportation – Karen Saunders (DPO)
  - Department of Transportation – Brenda Craig-Ellis (General Counsel)
  - Division of Motor Vehicles – Jill Dunn (General Counsel)
  - Division of Motor Vehicles – Joyce Abbott (APO)
- Department of Veterans Assistance – Mavery Davis (DPO)
- Chapter 30 Licensing Boards –Brenda Turley (Privacy Liaison)

Representing Other Constitutional Offices and Higher Education:

- State Auditor's Office – Mark Shelhammer
- Department of Education – Georgia Hughes-Webb
- Department of Education – Jeff Pitchford
- State Treasurer's Office – Kin Richardson
- State Treasurer's Office – Lisa Rutherford
- West Virginia School of Osteopathic Medicine – Jeffrey Shawver
- West Virginia School of Osteopathic Medicine – 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)

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

Jim Justice
Governor

John A. Myers
Cabinet Secretary

Mary Jane Pickens
Executive Director
Deputy Cabinet Secretary

December 29, 2017

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 first annual report on West Virginia's privacy program since the issuance of Executive Order No. 3-17.

This report reflects the successful integration of the State Privacy Office into BRIM's operations and the synergy created through collaborative risk management. The report is divided into three sections covering governance, risk management, and compliance.

With the input of privacy officers and others from across the Executive Branch, other constitutional offices and higher education, and the Chief Information Security Officer, we developed a strategic plan, covering years 2018 – 2020, which focuses our efforts on projects that matter most. Through governance measures, privacy risk management and legal compliance, we will strive to mature our privacy program. We will track our progress against this plan and include updates in future annual reports.

Maintaining our citizens' and employees' privacy is a priority for all of us. Thank you for your support.

Should you have any questions, please contact Chief Privacy Officer Sallie Milam at 304-766-2646 X 57624.

Very truly yours,

Mary Jane Pickens
Executive Director

INTRODUCTION

The State Privacy Office (SPO) manages the Executive Branch's Privacy 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 the leadership at the Board of Risk and Insurance Management (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) and Cybersecurity Administration Manager.

The SPO and the PMT efforts fall into three broad categories: accountability; risk management; and, compliance. The goal is to protect the personally identifiable information (PII) of the State's workforce and its citizens'. 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. This is demonstrated by authorizing and empowering the Executive Branch Privacy Program and State Privacy Office through Executive Order 3-17. Further, the Order affirms that "safeguarding the privacy of personal information collected, used, disclosed and maintained by the State is of the utmost importance to the citizens of the State. . ."

On May 18, 2017, Executive Order 3-17 was signed by Governor Justice, transferring oversight of the State's Privacy Program (Privacy Program) to the Director of BRIM from the WV Health Care Authority. The move to BRIM was in recognition of the complementary objectives and close working relationship the two organizations share in matters of privacy risk management and cyber-liability insurance.

The commitment to privacy by West Virginia's leadership is underscored by an annual proclamation of Data Privacy Day. 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.

The SPO launched the following accountability initiatives this year:

- Adoption of the American Institute of CPAs' (AICPA) Privacy Maturity Model, an internationally recognized framework for assessing strengths and weaknesses of a privacy program. It provides well-defined standards that are effective for advancing a privacy program.[1] Using this model, nine criteria were evaluated that fall under the privacy domain:

    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

- Development of a three-year strategic plan. The plan was based on a review of the nine criteria listed above and was completed with input from the PMT. The plan has six objectives and addresses five of the nine AICPA criteria:

    1) Increase the use of Privacy Impact Assessments (PIA). These 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. This one objective will improve two program criteria:

        - Infrastructure & Systems Management
        - Risk Assessment

    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]

    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. Recognizing the importance of incident management to reducing risk, the AICPA encourages rigorous responses to privacy incidents.

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

---

[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

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

5) Update and revise Executive Branch Privacy Policies and audit a representative sampling of agency privacy notices.

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

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:

- Working with leadership to support the development, issuance and implementation of Executive Order 3-17.

- Leading the bi-monthly PMT meetings, which provide a forum for information sharing, legislative updates, consensus building, security updates, open dialogue and training. The SPO sets the agendas for each meeting. In 2017, discussions and training included:

    - Vendor Assurance and Purchasing
    - Incident Response and Management (a year-long series)
    - Privacy Maturity Model
    - Strategic Plan Development
    - Payment Card Industry Awareness
    - Changes in Privacy Law and Regulation
    - Cybersecurity and Cyber Risk Management

- Advocating for the allocation of the appropriate level of dedicated workforce resources necessary to fulfill the privacy function.

- Training new Departmental Privacy Officers on roles and responsibilities.

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 this year supporting and enhancing risk management include:

[3] Dept. of Commerce. NIST. "Risk Management." Updated December 13, 2017. Accessed December 29, 2107. https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview.

- Revision of the PIA tool for both format and content. Questions were refined to create a more thorough record of data types collected by State information systems, enhancing data security in the process. 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 collection, use and storage factors; disclosure practices; and administrative, physical and technical controls.

- Revision of the privacy incident risk assessment process that is conducted to determine whether a breach has occurred. The new risk assessment provides a more targeted approach based on applicable law (e.g. WV State Breach Law, HIPAA/HITECH Act), and uses a qualitative approach incorporating ideas of reasonableness and sound judgement.

- Monthly 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 through 2018. 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.

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

- Additional standards for cyber/information security and privacy were added in 2017 to BRIM's existing Standards of Participation Program. These new standards were a collaboration of BRIM, the SPO, and the WVOT. They incentivize State organizations to adhere to Executive Branch privacy and security policies, including:

    - Confidentiality Agreements
    - Workforce Training
    - Record Retention
    - Data Classification
    - Encryption
    - Data Access and Audit
    - Vulnerability Scanning
    - Backup of Critical Information Systems

- Attendance at a learning event sponsored by the National Governor's Association on cyber threats and preparedness planning. The CPO, CISO and BRIM Deputy Director represented West Virginia at the event.

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

  According to the Ponemon Institute's 2017 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]

  The following training events and educational webinars were held by the SPO in 2017:

  - January – Data Privacy Day, which included an Incident Response Table-top Exercise
  - March – hosted a webinar on 2017 HIPAA Changes
  - April – provided on-site training for the Department of Environmental Protection, which covered the WV Privacy Program, Incident Management, PIAs and the Online Learning Management System
  - August – provided on-site training for the Department of Administration, Commerce Procurement Officers regarding privacy, managing vendor privacy and security risk and PIAs
  - August – Purchasing Conference presentation*: Purchasing – A Privacy Power House*
  - December – hosted a webinar on the HIPAA Compliance Checklist

COMPLIANCE

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

- 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.

[4] Ponemon Institute. "2017 Cost of Data Breach Study: Global Overview." June 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

- Management of the Executive Branch privacy incident response program. The SPO serves as a resource, throughout the duration of managing a privacy incident, from filing the initial report, through the investigation, to resolution.

- Provided advice and consultation regarding privacy policies, procedures, laws, regulations, and best practices in project design and implementation across the Executive Branch.

- Provided advice and consultation regarding privacy and security terms in Executive Branch contracts.

- 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 is looking forward to 2018 and implementing the projects outlined in the strategic plan. Our commitment to protecting the privacy of the State's citizens and workforce remains high. Future annual reports will cover the progress made in further developing the Executive Branch's Privacy Program as measured by the nine criteria of the AICPA Privacy Program Maturity Model.

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. "2017 Cost of Data Breach Study: Global Overview." June 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN