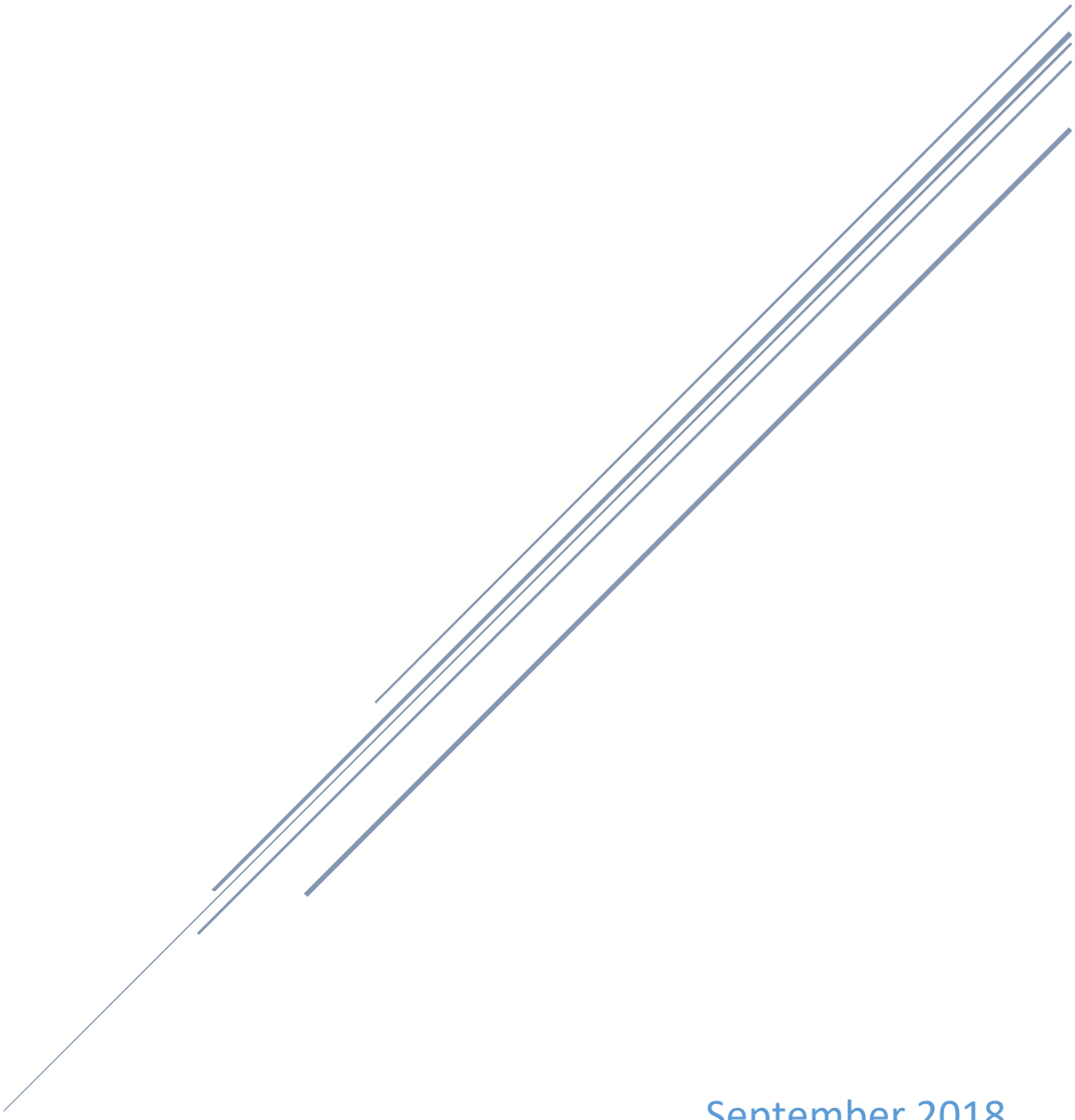
PERSONALLY IDENTIFIABLE INFORMATION WORKING GROUP STRATEGIC PLAN

Chair: Dewand Neely | Co-Chair: Valita Fredland



September 2018
Indiana Executive Council on Cybersecurity

Personally Identifiable Information Working Group Plan

Contents

Committee Members

Committee Members

Name	Organization	Title	Workgroup Position	IECC Membership Type
Dewand Neely	State of Indiana	Chief Information Officer	Chair	Voting
Ted Cotterill	State of Indiana	Chief Privacy Officer	Chair Proxy	Advisory
Valita Fredland	Indiana Health Information Exchange	VP – General Counsel & Privacy Officer	Co-Chair	Advisory
Doug Swetnam	Indiana Office of Attorney General	Section Chief – Data Privacy & Identify Theft Unit	Full Time	Voting Proxy
Tony Chu	Department of Revenue	Chief Information Security Officer	Full Time	Advisory
Mitch Parker	IU Health	Chief Information Security Officer	Full Time	Advisory
Leon Ravenna	KAR Auction Services	Chief Information Security Officer	Full Time	Advisory
Luke Britt	State of Indiana	Public Access Counselor	Full Time	Advisory
Ashley Schenck	Indiana Management Performance Hub	Director of Engagement & Analytics	Full Time	Advisory
Cliff McCullough	Family and Social Services Administration	Chief Privacy Officer	Full Time	Advisory
Chuck Cohen	Indiana Intelligence Fusion Center	Executive Director	Full Time	Voting Proxy
Dom Caristi	Ball State University	Professor of Telecommunications	Full Time	Advisory
Matt Odum	Briljent	President	Full Time	Advisory
Richard Braidich	RCR Technology	Chief Information Security Officer	Full Time	Advisory
John Lucas	Citizens Energy Group	VP of Information Technology	As Needed	Advisory
Lisa Berry-Tayman	CyberScout Solutions	Sr. Manager, Privacy and Information Guidance	Full Time	Advisory
Kim Metzger	Ice Miller	Partner	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Indiana Fair Information Practices Act, Ind. Code Ch. 4-1-6
    - http://iga.in.gov/legislative/laws/2017/ic/titles/004/#4-1-6
  - Indiana Access to Public Records Act, Ind. Code Ch. 5-14-3
    - http://iga.in.gov/legislative/laws/2017/ic/titles/005/#5-14-3
  - Indiana Disclosure of Security Breach Act, Ind. Code Art. 24-4.9
    - http://iga.in.gov/legislative/laws/2017/ic/titles/024/#24-4.9
  - Indiana Professional Services Contract Template
    - http://www.in.gov/idoa/files/Professional%20Services%20Contract%20Template%202017.docx
  - Indiana Additional Terms and Conditions, Software as a Service Engagements
  - State of Indiana Information Privacy Policy
  - NIST Privacy Program
    - https://www.nist.gov/privacy
  - NIST SP 800-53, Revision 5 (DRAFT), *Security and Privacy Controls for Information Systems and Organizations*
    - https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf
  - NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
    - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf
  - OMB Circular No. A-130 Revised
    - https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
  - OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
    - https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf
  - GAO Report, *Information Security: Protecting Personally Identifiable Information*
    - https://www.gao.gov/new.items/d08343.pdf
  - Privacy Act of 1974, 5 U.S.C. § 552a
    - https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf
  - E-Government Act of 2002
    - https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
  - FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*
    - https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
  - IAPP Glossary of Privacy Terms
    - https://iapp.org/resources/glossary/

- SANS CIS Critical Security Controls
  - https://www.sans.org/security-resources/posters/20-critical-security-controls/55/download

- **Research Findings**
  - The goal of defining "personally identifiable information" (PII) for use by a broad collection of individuals and entities presents a challenging task. This is due to the fact that there are many generally-applicable legal and policy definitions that include a similar set of data elements. For example, the State of Indiana's commercial data breach statute characterizes personal information as an unmasked social security number or first and last name with additional unmasked identifiers like a credit card number or driver's license number.[1] While this and similar PII characterizations are good candidates for use across multiple sectors, the US Office of Management and Budget defines PII as "…information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[2] This definition is particularly useful because it "…is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified."[3]
  - Laws like Children's Online Privacy Protection Act (COPPA), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), and their related administrative rules provide more specifically-applicable definitions which apply depending on the source of the information. Furthermore, certain acts provide de-identification methodologies that, if followed, allow the maintaining entity to make otherwise confidential information available publicly. One such example relates to the de-identification of protected health information. The rule allows for broader access to and use of the de-identified information if the following occurs:
    - A person with appropriate knowledge of and experience with generally accepted principles and methods for rendering information not individually identifiable… determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual…[4]
    - This rule acknowledges what is known as the "mosaic effect" whereby de-identified information can be combined with other available information to re-identify an individual. In this case, the definition of PII may be expanded to include other information that may be reasonably available to an anticipated recipient.

[1] Ind. Code § 24-4.9-2-10.
[2] OMB Memorandum M-07-16.
[3] GSA Policy and Procedure CIO P 2180.1.
[4] 45 CFR §164.514(b)(1).

- The current state of PII is one of change. The ability to re-identify an individual through the use of disparate, publicly-available datasets is real. As a result, the very definition of PII is in flux. A number of existing privacy regulations are cited above as "Research Conducted". While these are intended to protect the privacy of PII, many do so based upon possible historical use cases like the administration of a benefits program. Newer business intelligence technology offerings allow organizations to leverage information to make better-informed decisions and, while such use may fall within the spirit of these laws, there are few express allowances to be found. More and more, government is working to keep pace with emerging technologies, ensuring that the regulatory apparatus provides adequate protections to individuals while leaving room for innovation.
- To further complicate the matter, emerging technologies like Blockchain and related distributed ledger technologies have been discussed as potential solutions to the maintenance and exchange of high-value information. If applied to common PII maintenance and exchange scenarios, this decentralized maintenance of information presents such a significant departure from existing centralized models that related efforts would have to receive regulatory approval as pilot projects or run the risk of violating the law. In addition, there would need to be a shared governance model and auditing for distributed, decentralized systems to ensure integrity.

- **Final Deliverable**
  - Indiana PII Guidebook that will:
    - Define PII
    - Characterize the current state
    - Identify related regulations
    - Identify best practices across all sectors
    - Address potential future developments
    - Provide sample pragmatic policies and practices that, if followed, allow any Indiana business to implement the cybersecurity and risk mitigation practices identified by the PII Working Group

- **Additional Notes**
  - All referenced Research Conducted is available via the embedded link or as an attachment to this document.

- **Attachments**
  - State of Indiana Additional Terms and Conditions – SaaS
  - State of Indiana Information Privacy Policy

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. **IU Health:**
        i. Centers for Medicare & Medicaid Services (CMS) has released several guidance documents and programs on cybersecurity.
        ii. The Health Information Management Society (HIMSS) currently offers a comprehensive cybersecurity education program, as does the American Hospital Association (AHA), and American Health Information Management Association (AHIMA). In addition, the National Health Information Sharing and Advisory Center (NH-ISAC) also offers guidance to organizations, as does Infragard. HITRUST, which is a for-profit organization, is also popular with many large health systems and payers. HITRUST provides guidance and a security framework (HITRUST Common Security Framework or CSF).
        iii. However, much of this education is focused on either the basics or is aimed at highly sophisticated organizations, which is not the majority of healthcare.
    b. **Department of Revenue (DOR):**
        i. Provided annual awareness training to all employees, contractors, temps, vendors; facilitated business continuity and incident response exercises; and disseminated notifications about real-world security events, issues and best practices to the entire agency.
    c. **KAR Auction:**
        i. We cannot speak for the area in general; however, most cybersecurity programs are realistically less than 5 years old and have focused on “don’t click on the link”. The real issue here is critical thinking and how to discern what is being asked. For instance, you probably do not have a rich uncle elsewhere in the world that wants to give you money.
    d. **Citizens Energy:**
        i. We have done a significant amount of this to the BOD, and to Senior management through Risk Management efforts.
    e. **Briljent:**
        i. Very little, small business responds to the market at a rate that aligns with their budgets.
        ii. We have updated our annual user training and continue to push out updates to patch for new vulnerabilities.
    f. **RCR Technology:**
        i. We have developed multiple education PowerPoints that outline the key security issues and provided training to key developer areas.
        ii. Security resources continue to attend local and nearby security conferences whenever possible.
        iii. Completed all of the Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (Mars-e) version 2 security requirements which are **very** extensive.
        iv. We continue to assess and enhance all areas of security maturing our security stance over time.

v. We perform external penetration testing and run numerous other tools to assess the vulnerability of our systems from inside and outside the network.
vi. We perform our own personal assessments of cybersecurity that are based on industry knowledge and expertise as well as a variety of industry known methodologies.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. **IU Health:**
        i. Currently we believe those to be the continuing maintenance and upgrading of systems to protect against new and emerging threats, the abundance of legacy systems, the continuing issues with workflows, the lack of consistent training and education, and the economic pressures causing a de-emphasis on cyber due to having to keep the lights on in many organizations.
    b. **DOR:**
        i. External threats, malicious insiders, employees who fall for social engineering schemes, and sensitive data outside of the State's protected zone.
    c. **KAR Auction:**
        i. Unknowledgeable staff and weak technical controls for user-based activity. For example, protecting from inbound emails, web filtering, etc.
    d. **Citizens Energy:**
        i. We typically store a significant amount of PII to include social security numbers (SSN), banking information, and medical records.
    e. **Briljent:**
        i. As a small business, we are a hub of information for our employees and their families. Banking, medical, PII, passwords, network activity, etc. are all vulnerabilities that need to be considered.
    f. **RCR Technology:**
        i. The largest vulnerabilities are ones that are owned by the Indiana Office of Technology (IOT)
        ii. We are not able to update without their concurrence and support, and in some cases funding. This is not blaming them, only that they own and manage a lot of the essential infrastructure.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. **IU Health:**
        i. The need to provide basic education that is relevant to organizations to show them how to protect, as opposed to the constant emphasis on data breaches.
    b. **DOR:**
        i. Funding and manpower to support security assessments and implementation of security enhancements.
    c. **KAR Auction:**
        i. Encryption or pseudo anonymization

d. **Citizens Energy:**
    i. We believe medical records. HIPPA does not have any fines for violations. They leave this to the States. Indiana does not have any strong regulation to ensure compliance with HIPPA. In addition, Indiana Health Information Exchange (IHIE) is not regulated, and does not allow owners of the data in their database opt out. When one is able to opt out of the IHIE database, the data is not entirely removed; rather, it is only restricted from select searches and/or usage.
e. **Briljent:**
    i. Being secure with minimal budget and expertise
    ii. Intrusion detection
f. **RCR Technology:**
    i. Funding for security resources and expertise building through external training boot camps and conferences
    ii. Lack of a consolidated security information and event management tool that collects and combines all potential security events along with correlating all security data in one tool throughout the State's network.

4. What federal, state, or local cyber regulations is your area beholden to currently?

a. **IU Health:**
    i. We are required to follow the HIPAA Privacy and Security Rules, HITECH Act, Stark Act, and a number of state and local laws.
b. **DOR:**
    i. Internal Revenue Service (IRS) publication 1075, National Institute of Standards and Technology (NIST) special publication 800-53 and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), State code, and state agency policy and standards.
c. **KAR Auction:**
    i. HIPAA, Telephone Consumer Protection Act (TCPA), COPPA, General Data Protection Regulation (GDPR), Personal Information Protection and Electronic Documents Act (PIPEDA), Freedom of Information and Protection of Privacy Act (FIPPA), etc.
d. **Citizens Energy:**
    i. Strong state laws on PII. The definition of PII is somewhat vague and does not stay current with data being kept by businesses.
e. **Briljent:**
    i. We have audits of our systems by the Centers for Medicare and Medicaid Services to ensure compliance because we are a federal contractor. That is rare for a business our size outside of the niche of government contractors.
    ii. Not all of our work is affected by it, but we are primarily concerned about HIPAA due to the nature of our client work.
f. **RCR Technology:**
    i. CMS Mars-e v2 requirements

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. **IU Health:**
        i. We have highlighted the NH-ISAC Threat Intelligence Committees (TIC) and Cyberfit programs as great examples for how multiple organizations can work together to identify, classify, and mitigate threats across a large population.
        ii. We have also discussed how organizations are already self-organizing, specifically with Jennings Aske's work at Columbia/NYP.
    b. **DOR:**
        i. The Information Security Research and Education (INSuRE) program researches and seeks solutions to hard security problems. INSuRE members are the US Intelligence Community, US National Laboratories, US universities and colleges that include Purdue, and State government organizations that include IOT.
    c. **KAR Auction:**
        i. We would look at GDPR as an indication of where privacy or safeguarding sensitive information is going.
    d. **RCR Technology:**
        i. NIST Cybersecurity framework, https://www.nist.gov/cyberframework
        ii. Center for Internet Security (CIS) Critical Security Controls, https://www.cisecurity.org/controls/
        iii. SANS Institute top 20 critical security controls, https://www.sans.org/security-resources/posters/20-critical-security-controls/55/download

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. **DOR:**
        i. DOR white paper defining sensitive data that DOR must protect
        ii. DOR Protection of Taxpayer Information Job Aid
        iii. Department of Homeland Security (DHS) Factsheet on Safeguarding PII
        iv. DHS Handbook for Safeguarding Sensitive PII
    b. **RCR Technology:**
        i. Most of what is available is good, but not useful in validating true expertise and experience.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. **IU Health:**
        i. They are currently utilizing the same sources we are, plus also self-organizing as part of emergency management to address these issues.
    b. **DOR:**
        i. The IRS requires anyone receiving Federal Tax Information (FTI) to receive security awareness training, additional security training for specific roles, and contingency and incident response training for pertinent personnel.

c. **Briljent:**
    i. As many others do, we comply with contract regulations and hope that suits the rest of our business functions well.
d. **RCR Technology:**
    i. They are provided with sizable budgets for security conferences, training and boot camps. This is essential.

8. What does success look like for your area in one year, three years, and five years?

a. **IU Health:**
    i. Year 1:
        1. Begin developing a pilot program modeled after NH-ISAC's TICs to collaborate across multiple institutions to address security issues and provide a means for healthcare organizations to contact us to report potential issues. Beginnings of a communication plan designed to reach out to healthcare providers.
    ii. Year 3:
        1. Expansion of the program to have more dedicated staff and interaction with providers. More proactive education, collaboration with other states, and organizations such as NH-ISAC, Infragard, and DHS to provide cybersecurity awareness.
    iii. Year 5:
        1. Having this program as part of normal business of the State.
b. **DOR:**
    i. Year 1: Implement the performance of annual security assessments and security controls for severe and significant findings.
    ii. Year 3 & 5: Help vendors, partners, and tax e-filing community become compliant with DOR security; improve agency access controls, data security, and vulnerability management; and normalize annual business continuity/disaster recovery planning and testing.
c. **Briljent:**
    i. Compliance with state and federal programs in coalition with comparable businesses to share cost and expertise
    ii. Preventing a cybersecurity incident outright, or preventing a cybersecurity incident from having a business impact.
d. **RCR Technology:**
    i. This is very difficult to quantify, but success is measured by at least two key metrics:
    ii. Security assessment performed against the network and key resources. The assessment should show that all High and most Medium level risks are mitigated and/or actions are in place to compensate and/or address these risks. Compensating and/or addressing the risks should happen within a reasonable timeframe, to a degree that is understood, and approved by the State. Key factors the security assessment would need to include are the industry known security threats that exist.
    iii. All compliance requirements in the area of cybersecurity are achieved, and/or plans of action are approved

9. **What are the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. **IU Health:**
        i. There needs to be a concerted effort to reach out to specific medical providers to specifically address what they need to do to increase security. People are very aware of the need for cybersecurity. The specific guidance that they need to be secure has been either too specific or lacking.
    b. **DOR:**
        i. The public should be apprised that DOR continuously implements tools and processes to bolster cybersecurity to protect their information, which may appear inconvenient to them. For example, we may require taxpayers logging into our applications to increase the length and complexity of their passwords.
    c. **KAR Auction:**
        i. Realistically, the biggest area is to help people understand how to protect themselves. Does that phone application you are installing really need geo-location tracking services, do you really need to give up your contacts? How to turn off base services on your Android or iOS.
    d. **Briljent:**
        i. We believe there is a serious need for public outreach and education around cybersecurity so that risk can be further understood and personal decisions made with that risk in mind.
        ii. More online training provided by the State would help.
    e. **RCR Technology:**
        i. Provide the funding for at least 2 major security conferences and 2 security training classes per year.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. **IU Health:**
        i. According to the 2015 Bureau of Labor Statistics (BLS), 9.0% of the total workforce in Indiana is in healthcare.
        ii. There are no clear statistics as to how much of that section workforce is cybersecurity related.
        iii. IU Health employs approximately 30,000 people. Approximately 550 personnel work in information technology (IT), which is approximately 2% of the workforce. Of that, 20 staff members are dedicated to cybersecurity full-time. Which is approximately 0.07% of the total workforce.
        iv. According to a Frost & Sullivan report, 30% of healthcare hiring managers plan to increase staff by 20% or more, and 9% want to hire between 16% and 20% additional personnel.

v. However, because of a lack of risk assessments and actual planning, according to the May 2017 Health Care Industry Cybersecurity Task Force task report, this number is not even close to accurate. Further analysis of BLS 2016-2026 statistics, in combination with the sources indicating that we need hundreds of thousands of jobs to fill cybersecurity vacancies, indicate that the number is closer to 50,000 in the US.
vi. The issue is not cybersecurity jobs, it is getting people to understand cybersecurity and exercise due diligence.

b. **DOR:**
   i. Total DOR Workforce as of December 2017: 751. We have 659 FTEs and 92 contractors.
   ii. Total DOR Cybersecurity Staff: 6
   iii. Total DOR Cybersecurity Staff shortfall: 0

c. **KAR Auction:**
   i. We cannot answer for this area, but the cybersecurity footprint of any company is remarkably small. Average companies that have security departments are relatively small in comparison to large corporations (e.g. Target, Home Depot, and Equifax). Because many businesses have little understanding of cybersecurity, this may account for the small to non-existent dedicated security personnel employed in smaller Indianapolis businesses.

d. **RCR Technology:**
   i. Workforce: 120 people
   ii. Cybersecurity: 1.5 people
   iii. We need 2 people

11. What do we need to do to attract cyber companies to Indiana?

a. **IU Health:**
   i. Advertise and leverage the educational advantage that Indiana has with IU, Purdue, IUPUI, Rose-Hulman, and Notre Dame. Two of the best and most well-connected cyber programs in the country are here, and there are already a number of tech companies, specifically Salesforce, taking full advantage of that. Facilitating business development and encouraging companies to locate offices and/or staff here based on the availability of top-level graduates, quality of living, and low cost would greatly assist.

b. **KAR Auction:**
   i. Build the community. Security people are insular and do not talk. We need them to be comfortable to share information, mentor and lead. Additionally, we need to pull in some security-based companies. The smaller local boutique firms are great, but it is not a state focus as it is not well understood.

c. **Citizens Energy:**
   i. Grow the corporate headquarters in Indiana. This creates the need for cybersecurity companies.

d. **Briljent:**
   i. Show that Indiana has strong growth in the technology sector.

12. What are your communication protocols in a cyber emergency?

a. **IU Health:**
   i. We follow the Hospital Incident Command System (HICS) to escalate incidents. We now have coordinated communication with multiple agencies and will follow the same protocols as a standard multi-site incident. Ultimately, a multidisciplinary approach in healthcare is needed that utilizes HICS as patient safety has to be paramount.

b. **DOR:**
   i. We communicate based on our formalized process of identifying, analyzing, responding to, and recovering from incidents to include cyber emergencies.

c. **KAR Auction:**
   i. Electronic, cell-based

d. **Briljent:**
   i. Email is the preferred method of communication. We generally notify all users, even those that may not be directly affected by a cybersecurity threat.

e. **RCR Technology:**
   i. The State has a planned outlined.

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. **IU Health:**
   i. Focus on assessing risk, and helping people understand what to do to address it. The issue is that we do not focus on the fundamentals, and need to treat cybersecurity as part of the business rather than something to address separately. The more we focus on it as a separate discipline, the less we will be able to attack root causes of many of these issues.

b. **DOR:**
   i. Defense in-depth: an information assurance concept in which multiple layers of security controls are placed throughout an information technology system
   ii. Initial and annual security awareness training
   iii. Phishing testing

c. **Briljent:**
   i. Much of the federal guidance is applicable at the state level as well.

Deliverable: Indiana PII Guidebook

Deliverable: Indiana PII Guidebook

General Information

1. **What is the deliverable?**
    a. The Indiana PII Guidebook will consist of the following:
        i. Define PII
        ii. Characterize the current state
        iii. Identify related regulations
        iv. Identify best practices across all sectors
        v. Address potential future developments
        vi. Provide sample pragmatic policies and practices that, if followed, allow any Indiana business to implement the cybersecurity and risk mitigation practices identified by the PII Working Group

2. **What is the status of this deliverable?**
    a. In-progress; 25% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Enhanced knowledge of what we should be protecting.
    b. This provides an actionable blueprint to Hoosier businesses to protect the privacy of individually-identifiable information.
    c. Provide quick-reference visibility into best practices.
    d. Ensuring a well-rounded output by the PII Working Group.
    e. Providing context around potential result of technological advancement, today's policy decisions, etc.
    f. Recognition of current posture is important to understand where we need to be.

6. **What metric or measurement will be used to define success?**
    a. All-encompassing definition and ease of application by end users.
    b. Generation of an all-encompassing reference list for PII Working Group use.
    c. Robust assessment of the current state.
    d. Usability by a broad swath of Hoosier businesses.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. All those who are working to define PII and those who would like context behind PII.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Unknown

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Sector-specific groups or all sectors will be engaged on an as-needed basis.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Any on an as-needed basis.

12. **Who should be main lead of this deliverable?**
    a. PII Working Group

13. What are the expected challenges to completing this deliverable?

a. Ensuring that definition has high utility to various sectors.
b. Providing an end-product that is sufficiently all encompassing so as to be valuable for a large number of users.
c. Accurately capturing all PII best practices.
d. Difficult to capture all regulations across all sectors.
e. Difficult to tell the future in any space, especially technology.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Define PII	Richard Braidich & Tony Chu	25%	End of Q4, 2018	
Characterize the current state	Ashley Schenck	25%	End of Q4, 2018	
Identify related regulations	Ted Cotterill	25%	End of Q4, 2018	
Identify best practices across all sectors	Valita Fredland	25%	End of Q4, 2018	
Address potential future developments	Leon Ravenna & Mitch Parker	25%	End of Q4, 2018	
Provide sample pragmatic policies and practices that, if followed, allow any Indiana business to implement the cybersecurity and risk mitigation practices identified by the PII Working Group	Dom Caristi	25%	End of Q4, 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No
b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. A cross-sector body of subject-matter experts is required to form an understanding of Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the body of talent to stay on the forefront of the cyber risk environment. To provide Hoosiers with a foundational understanding of that which we intend to protect, the Personally Identifiable Information Working Group will create the Indiana PII Guidebook. This is intended to do the following:
    i. define PII
    ii. characterize the current state
    iii. identify related regulations
    iv. identify best practices across all sectors
    v. address potential future developments; and
    vi. provide sample pragmatic policies and practices that, if followed, allow any Indiana business to implement the cybersecurity and risk mitigation practices identified by the PII Working Group.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable compliments the work of other components of the Indiana Executive Council on Cybersecurity by providing both a foundational understanding of personally identifiable information as well as articulating how the definition can be applied to specific information maintained by any number of Hoosier businesses.
b. Costs associated with the enhanced knowledge regarding PII are unknown.

19. What is the risk or cost of not completing this deliverable?

a. This deliverable will be completed by the PII Working Group. If it were not completed, Hoosiers would not realize the benefit of added knowledge about the core data elements that must be protected.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. A completed and approved Indiana PII Guidebook defines the success of this deliverable.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Unknown. At this time, PII Working Group members remain engaged and related tactics are well defined. Ownership of each has been assigned.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. N/A

b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. The PII Working Group is striving to provide a Guidebook that provides a definition of PII that can be leveraged by all business sectors across Indiana. As such, the definition is unlikely to be limited to fixed data elements that are commonly thought of as direct identifiers. It is more likely that the definition will provide a framework or PII-related decision tree that can be applied to any business situation.

b. The avoidance of a fixed-element definition will lend itself to a more lasting benefit for Hoosiers. However, periodic review and revision by subject matter experts may be required to ensure that the Indiana PII Guidebook remains relevant.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. The PII Working Group is made up of members that maintain a depth and breadth of knowledge in the realm that is unparalleled across the State of Indiana. Members have consulted bodies of knowledge on the subject and intend to communicate that knowledge in a consumable way that enables real action by Hoosiers.

27. Can this deliverable be used by other sectors?

a. Yes.

b. **If Yes, please list sectors**

i. All.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. IECC lead-agency communications directors should be made aware of the Indiana PII Guidebook and align with an appropriate marketing strategy.

Evaluation Methodology

Objective 1: IECC PII Working Group develop an Indiana PII Guidebook for government and general public by the end of Q1, 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Department of Revenue PII Research Responses
- State of Indiana Additional Terms and Conditions – Software as a Service (SaaS)
- State of Indiana Information Privacy Policy

Department of Revenue (DOR)

PII Research Responses

2018

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

COMMITTEE AND WORKING GROUP QUESTIONNAIRE – RESEARCH PHASE

Instructions: As your committee or working group is in the Research Phase, it is important we work with other committees and working groups to get the information your team will need to be successful. Please answer the questions the best you can.

*Provide your questions and answers to MosleyCLM@iot.in.gov no later than **Jan. 10, 2018.***

Committee/Working Group:	Personally Identifiable Information Working Group
Person Submitting Summary:	Tony Chu
Email of Person Submitting:	TChu@dor.in.gov

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. **Department of Revenue (DOR):**
        i. Provided security awareness training to all full time employees (FTE), contractors, temps, and vendors at on-boarding and annually thereafter. This training apprises employees of the data they must protect, and the methods by which they must be protected.
        ii. Led a Continuity of Operations plan exercise in 2014 and the next one is projected for 2018.
        iii. Trained and exercised the DOR Incident Response team and plan annually.
        iv. Sent periodic e-mails and published articles in agency publications apprising DOR-all of security issues and best security practices.
        v. Sent e-mails to DOR-all apprising them of urgent real-world security issues, and how to address them (e.g., phishing messages and phone-based social engineering attacks)

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. **DOR:**
        i. External threats: State and non-state cyber actors, cybercriminals, cyberterrorists, etc.
        ii. Malicious insiders
        iii. Employees who fall for social engineering schemes
        iv. Servers containing sensitive data that reside outside of the state's protected zone (PZ)

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. **DOR:**
        i. Internal Revenue Service (IRS) Publication 1075
        ii. National Institute of Standards and Technology (NIST) Special Publication 800-53: Using Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) for detailed security assessments
        iii. Indiana Code and policies
        iv. IOT policies and standards
        v. DOR policies and procedures

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. **DOR:**
        i. All other state departments of revenue/taxation that receive Federal Tax Information (FTI) are required by IRS to provide:
            1. Security awareness training to all employees
            2. Role-based training to personnel based on assigned security roles and responsibilities
            3. Contingency training to personnel responsible for recovering backup copies of FTI
            4. Incident response training to personnel responsible for handling and reporting security events

8. **What does success look like for your area in one year, three years, and five years?**
    a. **DOR:**
        i. Year 1:
            1. Conduct security assessments
            2. Implement security controls address severe and significant vulnerabilities and threats
        ii. Year 3:
            1. DOR, its vendors, partners, and e-filing tax community comply with DOR security requirements
            2. Work towards the following goals
                a. All sensitive DOR servers reside in the state's PZ
                b. DOR servers reside in appropriate network segments

c. All sensitive DOR data within the state network is encrypted at rest and in motion
d. DOR users have least privileged access
e. Security patching is done immediately
f. Continuity of Operations (COOP) and Disaster Recovery (DR) plans are developed, appropriately resourced, and successfully tested

iii. Year 5:
1. Achieve the following goals
a. All sensitive DOR servers reside in the state's PZ
b. DOR servers reside in appropriate network segments
c. All sensitive DOR data within the state network is encrypted at rest and in motion
d. DOR users have least privileged access
e. Security patching is done immediately
f. COOP and DR plans are developed, appropriately resourced, and successfully tested

12. What are your communication protocols in a cyber emergency?

a. **DOR:**
i. DOR employee, Indiana Office of Technology (IOT) employee, or anyone else identifies and reports suspicious activities to DOR Security Team.
ii. DOR security team assesses and analyzes the situation to determine if there is an emergency.
iii. DOR security team, upon DOR chief information officer (CIO) approval, takes immediate action as necessary to stop the perpetuation of damage.
iv. DOR security team develops multiple courses of action (COA) to address remaining security concerns and to recover from the event. They then present the COAs to other members of the DOR incident response team comprising of DOR chief operating officer, DOR chief information officer, DOR inspector general, DOR legal team, DOR communications team, and IOT chief information security officer.
v. DOR incident response team decides on a single course of action.
vi. DOR incident response team briefs DOR commissioner on the situation, actions taken, and proposed COA.
vii. DOR commissioner approves COA
viii. DOR incident response team works with IOT to execute the approved COA.

State of Indiana Additional Terms and Conditions

Software as a Service (SaaS)

March 2017

State of Indiana Additional Terms and Conditions
Software as a Service Engagements

Exhibit 1 to the Contract between the State acting through [agency name] and the Contractor.

DEFINITIONS

Data means all information, whether in oral, written, or electronic form, created by or in any way originating with the State, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or that in any way originated with the State, in the course of using and configuring the Services.

Data Breach means any actual or reasonably suspected unauthorized access to or acquisition of Encrypted Data.

Encrypted Data means Data that that is required to be encrypted under the contract and Statement of Work.

Indiana Office of Technology means the agency established by Ind. Code § 4-13.1-2-1.

Information Security Framework means the State of Indiana's written policy and standards document governing matters affecting security and available at http://www.in.gov/iot/2339.htm.

Security Incident means any actual or reasonably suspected unauthorized access to the contractor's system, regardless of whether contractor is aware of a Data Breach. A Security Incident may or may not become a Data Breach.

Service(s) means that which is provided to the State by contractor pursuant to this contract and the contractors obligations under the contract.

Service Level Agreement means a written agreement between both the State and the contractor that is subject to the terms and conditions of this contract. Service Level Agreements should include: (1) the technical service level performance promises (i.e. metrics for performance and intervals for measure); (2) description of service quality; (3) identification of roles and responsibilities; (4) remedies, such as credits; and (5) an explanation of how remedies or credits are calculated and issued.

Statement of Work means the written agreement between both the State and contractor attached to and incorporated into this contract.

TERMS

1. Data Ownership: The State owns all rights, title, and interest in the Data. The contractor shall not access State user accounts or Data, except: (1) in the normal course of data center operations; (2) in response to Service or technical issues; (3) as required by the express terms of this contract, applicable Statement of Work, or applicable Service Level Agreement; or (4) at the State's written request.

Contractor shall not collect, access, or use Data except as strictly necessary to provide Service to the State. No information regarding State's use of the Service may be disclosed, provided, rented, or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this contract.

2. Data Protection: Protection of personal privacy and Data shall be an integral part of the business activities of the contractor to ensure there is no inappropriate or unauthorized use of Data at any time. To this end, the contractor shall safeguard the confidentiality, integrity, and availability of Data and shall comply with the following conditions:

a. The contractor shall implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, or theft of Data. Contractor shall implement and maintain heightened security measures with respect to Encrypted Data. Such security measures shall be in accordance with Indiana Office of Technology practice and recognized industry practice, including but not limited to the following:

1. Information Security Framework; and

2. Indiana Office of Technology Cloud Product and Service Agreements, Standard ID: IOT-CS-SEC-010.

b. All Encrypted Data shall be subject to controlled access. Any stipulation of responsibilities shall be included in the Statement of Work and will identify specific roles and responsibilities.

c. The contractor shall encrypt all Data at rest and in transit. The State may, in the Statement of Work, identify Data it deems as that which may be publicly disclosed that is not subject to encryption. Data so designated may be maintained without encryption at rest and in transit. The level of protection and encryption for all Encrypted Data shall meet or exceed that required in the Information Security Framework.

d. At no time shall any Data or processes — that either belong to or are intended for the use of State — be copied, disclosed, or retained by the contractor or any party related to the contractor for subsequent use in any transaction that does not include the State.

e. The contractor shall not use any information collected in connection with the Services for any purpose other than fulfilling its obligations under the contract.

3. Data Location: Storage of Data at rest shall be located solely in data centers in the United States and the contractor shall provide its Services to the State and its end users solely from locations in the United States. The contractor shall not store Data on portable devices, including personal laptop and desktop computers. The contractor shall access Data remotely only as required to provide technical support. The

contractor shall provide technical user support on a 24/7 basis unless specified otherwise in the Service Level Agreement.

4. Notice Regarding Security Incident or Data Breach:

a. Incident Response: contractor may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries, and seeking external expertise as mutually agreed upon, defined by law, or contained in the contract. Discussing Security Incidents and Data Breaches with the State must be handled on an urgent basis, as part of contractor's communication and mitigation processes as mutually agreed upon in the Service Level Agreement, contained in the contract, and in accordance with IC 4-1-11 and IC 24-4.9 as they may apply.

b. Security Incident Reporting Requirements: The contractor shall report a Security Incident to the State-identified contact(s) as soon as possible by telephone and email, but in no case later than two (2) days after the Security Incident occurs. Notice requirements may be clarified in the Service Level Agreement and shall be construed in accordance with IC 4-1-11 and IC 24-4.9 as they may apply.

c. Data Breach Reporting Requirements: If a Data Breach occurs, the contractor shall do the following in accordance with IC 4-1-11 and IC 24-4.9 as they may apply: (1) as soon as possible notify the State-identified contact(s) by telephone and email, but in no case later than two (2) days after the Data Breach occurs unless a shorter notice period is required by applicable law; and (2) take commercially-reasonable measures to address the Data Breach in a timely manner. Notice requirements may be clarified in the Service Level Agreement. If the Data involved in the Data Breach involves protected health information, personally identifying information, social security numbers, or otherwise confidential information, other sections of this contract may apply. The requirements discussed in those sections must be met in addition to the requirements of this section.

5. Responsibilities Regarding Data Breach: This section applies when a Data Breach occurs with respect to Encrypted Data within the possession or control of the contractor.

a. The contractor shall: (1) cooperate with the State as reasonably requested by the State to investigate and resolve the Data Breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document and provide to the State responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the Services, if necessary.

b. Unless stipulated otherwise in the Statement of Work, if a Data Breach is a result of the contractor's breach of its contractual obligation to encrypt Data or otherwise prevent its release as reasonably determined by the State, the contractor shall bear the costs associated with: (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators, or others required by federal and/or state law, or as otherwise agreed to in the Statement of Work; (3) a credit monitoring service required by federal and/or state law, or as otherwise agreed to in the Statement of Work; (4) a website or a toll-free number and call center for affected individuals required by federal and/or state law — all of which shall not amount to less than the average per-record per-person cost calculated for data breaches in the United States (in, for example, the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the Data Breach); and (5) complete all

corrective actions as reasonably determined by contractor based on root cause and on advice received from the Indiana Office of Technology. If the Data involved in the Data Breach involves protected health information, personally identifying information, social security numbers, or otherwise confidential information, other sections of this contract may apply. The requirements discussed in those sections must be met in addition to the requirements of this section.

6. Notification of Legal Requests: If the contractor is requested or required by deposition or written questions, interrogatories, requests for production of documents, subpoena, investigative demand or similar process to disclose any Data, the contractor will provide prompt written notice to the State and will cooperate with the State's efforts to obtain an appropriate protective order or other reasonable assurance that such Data will be accorded confidential treatment that the State may deem necessary.

7. Termination and Suspension of Service:

a. In the event of a termination of the contract, the contractor shall implement an orderly return of Data in a mutually agreeable and readable format. The contractor shall provide to the State any information that may be required to determine relationships between data rows or columns. It shall do so at a time agreed to by the parties or shall allow the State to extract its Data. Upon confirmation from the State, the contractor shall securely dispose of the Data.

b. During any period of Service suspension, the contractor shall not take any action that results in the erasure of Data or otherwise dispose of any of the Data.

c. In the event of termination of any Services or contract in its entirety, the contractor shall not take any action that results in the erasure of Data until such time as the State provides notice to contractor of confirmation of successful transmission of all Data to the State or to the State's chosen vendor.

During this period, the contractor shall make reasonable efforts to facilitate the successful transmission of Data. The contractor shall be reimbursed for all phase-out costs (i.e., costs incurred within the agreed period after contract expiration or termination that result from the transfer of Data or other information to the State). A reimbursement rate shall be agreed upon by the parties during contract negotiation and shall be memorialized in the Statement of Work. After such period, the contractor shall have no obligation to maintain or provide any Data and shall thereafter, unless legally prohibited, delete all Data in its systems or otherwise in its possession or under its control. The State shall be entitled to any post-termination assistance generally made available with respect to the Services, unless a unique data retrieval arrangement has been established as part of a Service Level Agreement.

d. Upon termination of the Services or the contract in its entirety, contractor shall, within 30 days of receipt of the State's notice given in 7(c) above, securely dispose of all Data in all of its forms, including but not limited to, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the State upon completion.

8. Background Checks: The contractor shall conduct a Federal Bureau of Investigation Identity History Summary Check for each employee involved in provision of Services: (1) upon commencement of the contract; (2) prior to hiring a new employee; and (3) for any employee upon the request of the State. The contractor shall not utilize any staff, including subcontractors, to fulfill the obligations of the

contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to one (1) year is an authorized penalty. The contractor shall promote and maintain an awareness of the importance of securing the State's information among the contractor's employees, subcontractors, and agents. If any individual providing Services under the contract is not acceptable to the State, in its sole opinion, as a result of the background or criminal history investigation, the State, in its sole option shall have the right to either: (1) request immediate replacement of the individual; or (2) immediately terminate the contract, related Statement of Work, and related Service Level Agreement.

9. Access to Security Logs and Reports: The contractor shall provide to the State reports on a schedule and in a format specified in the Service Level Agreement as agreed to by both the contractor and the State. Reports shall include latency statistics, user access, user access IP address, user access history, and security logs for all Data. The State's audit requirements shall, if applicable, be defined in the Statement of Work.

10. Contract Audit: The contractor shall allow the State to audit conformance to the contract terms. The State may perform this audit or contract with a third party at its discretion and at the State's expense.

11. Data Center Audit: The contractor shall perform an annual independent audit of its data center(s) where Data, State applications, or other State information is maintained. The contractor shall perform this independent audit at its expense and shall, upon completion, provide an unredacted version of the complete audit report to the State. (The contractor may redact its proprietary information from the unredacted version, however.) A Service Organization Control (SOC) 2 audit report or equivalent approved by the Indiana Office of Technology sets the minimum level of a third-party audit.

The State may perform an annual audit of contractor's data center(s) where Data, State applications, or other State information is maintained. The audit may take place onsite or remotely, at the State's discretion. The State shall provide to contractor thirty (30) days' advance notice prior to the audit. The contractor will make reasonable efforts to facilitate the audit and will make available to the State members of its staff during the audit. The State may contract with a third party to conduct the audit at its discretion and at the State's expense. If the contractor maintains Data, State applications, or other State information at multiple data centers, the State may perform an annual audit of each data center.

The parties agree that any documents provided to the State under this paragraph shall be deemed a trade secret of contractor and is deemed administrative or technical information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under the Indiana Access to Public Records Act, IC 5-14-3.

12. Change Control and Advance Notice: The contractor shall give notice to the State for change management requests. Contractor shall provide notice to the State regarding change management requests that do not constitute an emergency change management request at least two (2) weeks in advance of implementation. Contractor shall provide notice to the State regarding emergency change management requests no more than twenty-four (24) hours after implementation.

Contractor shall make updates and upgrades available to the State at no additional cost when contractor

makes such updates and upgrades generally available to its users. No update, upgrade, or other change to the Service may decrease the Service's functionality, adversely affect State's use of or access to the Service, or increase the cost of the Service to the State.

13. Security: The contractor shall, on an annual basis, disclose its non-proprietary system security plans or security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the contractor. For example: virus checking and port sniffing. The State and the contractor shall share information sufficient to understand each other's roles and responsibilities. The contractor shall take into consideration feedback from the Indiana Office of Technology with respect to the contractor's system security plans.

The parties agree that any documents provided to the State under this paragraph shall be deemed a trade secret of contractor and is deemed administrative or technical information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under the Indiana Access to Public Records Act, IC 5-14-3.

14. Non-disclosure and Separation of Duties: The contractor shall enforce role-based access control, separation of job duties, require commercially-reasonable nondisclosure agreements, and limit staff knowledge of Data to that which is absolutely necessary to perform job duties. The contractor shall annually provide to the State a list of individuals that have access to the Data and/or the ability to service the systems that maintain the Data.

15. Import and Export of Data: The State shall have the ability to import or export Data in piecemeal or in entirety at its discretion, with reasonable assistance provided by the contractor, at any time during the term of contract. This includes the ability for the State to import or export Data to/from other parties at the State's sole discretion. Contractor shall specify in the Statement of Work if the State is required to provide its' own tools for this purpose, including the optional purchase of contractor's tools if contractor's applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The contractor shall be responsible for the acquisition and operation of all hardware, software, and network support related to the Services being provided. The technical and professional activities required for establishing, managing, and maintaining the environments are the responsibilities of the contractor. Subject to the Service Level Agreement, the Services shall be available to the State at all times. The contractor shall allow the State to access and use the Service to perform synthetic transaction performance testing.

The contractor shall investigate and provide to the State a detailed incident report regarding any unplanned Service interruptions or outages. The State may terminate the contract for cause if, at its sole discretion, it determines that the frequency of contractor-preventable outages is sufficient to warrant termination.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to Services, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the contractor, and who may be involved in any application development and/or operations.

The contractor shall be responsible for the acts and omissions of its subcontractors, strategic business partners, or other entities or individuals who provide or are involved in the provision of Services.

18. Business Continuity and Disaster Recovery: The State's recovery time objective shall be defined in the Service Level Agreement. The contractor shall ensure that the State's recovery time objective has been met and tested as detailed in the Service Level Agreement. The contractor shall annually provide to the State a business continuity and disaster recovery plan which details how the State's recovery time objective has been met and tested. The parties agree that any documents provided to the State under this paragraph shall be deemed administrative or technical information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under the Indiana Access to Public Records Act, IC 5-14-3. The contractor shall work with the State to perform an annual disaster recovery test and take action to correct any issues detected during the test in a time frame mutually agreed upon between the contractor and the State in the Service Level Agreement.

The State's Data shall be maintained in accordance with the applicable State records retention requirement, as determined by the State. The contractor shall annually provide to the State a resource utilization assessment detailing the Data maintained by the contractor. This report shall include the volume of Data, the file formats, and other content classifications as determined by the State.

19. Compliance with Accessibility Standards: The contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the State.

20. State Additional Terms and Conditions Revision Declaration: The clauses in this Exhibit have not been altered, modified, changed, or deleted in any way except for the following clauses which are named below:_____

State of Indiana
Information Privacy Policy

September 2017

State of Indiana Information Privacy Policy

Version: 1 (9/15/17)

Contents

Purpose

The purpose of this Policy is to ensure that data maintained by the State of Indiana is kept and treated in accordance with applicable laws and regulations. This policy will provide guidance to State agencies as they work to maintain the privacy of those they serve.

Applicability

This Policy shall apply to all Government Information. Nothing contained in this Policy shall be construed to require an agency to expend funds for the sole purpose of obtaining compliance with this Policy. However, at such time as information technology systems are procured or altered, an agency shall consult with the MPH and shall make reasonable efforts to obtain compliance with this Policy.

Authority

This Policy is promulgated by the Indiana Management Performance Hub pursuant to IC 4-3-26-10(3).

Definitions

1. "APO" means an Agency Privacy Officer as discussed herein.
2. "CPO" means the Chief Privacy Officer of the state.
3. "Government information" has the meaning set forth in IC 4-3-26-7.
4. "IOT" means the Indiana Office of Technology established by IC 4-13.1-2-1.
5. "MPH" means the Indiana Management Performance Hub established by IC 4-3-26-8.
6. "Personal information" has the meaning set forth in IC 4-1-6-1(b).
7. "Policy" means this *State of Indiana Information Privacy Policy*.

Background

Through the daily operations of its agencies, the State of Indiana creates, maintains, and safeguards vast amounts of information relating to its citizens and the governing process. This data is a valuable asset in providing government services to the public as well as informing the policymaking process to ensure the best outcomes for the Hoosiers we serve. Ensuring that Government Information is maintained appropriately is of critical concern.

Policy

Maintaining the privacy of Government Information is ultimately the responsibility of all State agency employees as they create, capture, and store information in the course of their duties. To effectively maintain the privacy of Government Information, State agency employees must understand the content of the Government Information at issue and how that content affects the agency's privacy responsibilities.

The MPH seeks to establish a policy which recognizes and accounts for the relationship and linkage between privacy and security controls, enabling State agencies to more efficiently maintain the privacy of Personal Information. To do so, the MPH puts forth this Policy, which is adapted from *Best Practices: Elements of a Federal Privacy Program*, authored by the Federal CIO Council.[1]

The Policy includes six components, which are essential elements of an effective privacy management program. Those are leadership and accountability, privacy risk management and compliance documentation, information security, incident response, notice and redress for individuals, and privacy awareness.

Each is discussed in greater detail below.

Leadership & Accountability

The State of Indiana's success in the maintenance of individual privacy begins with leadership. IT systems can be built to accommodate varying levels of access, but it is top-down direction that will ensure diligence on the part of State employees. It is on those lines that the MPH recommends the appointment of an Agency Privacy Officer in each agency. As a part-time role, it is suggested that the APO be an individual serving as agency general counsel or records/compliance counsel, creating alignment with the day-to-day duties and the role of APO. The APO will work with the MPH and will be responsible for:

- Ensuring agency compliance with applicable State and Federal laws and regulations;
- Overseeing and coordinating agency privacy compliance efforts;
- Remaining abreast of legislative change regarding privacy in the agency's sphere of operation; and
- Collaborating with other APO's and the Chief Privacy Officer.

Housed in MPH, the CPO can serve as a liaison for intergovernmental, multi-agency, and public-private efforts that involve the privacy of Government Information.

The APO should have a foundational understanding of the Fair Information Practices Act at Ind. Code Ch. 4-1-6, the Access to Public Records Act at Ind. Code Ch. 5-14-3, and any statutes and rules that govern the Government Information at issue with more specificity. The CPO can assist APOs in the review and application of these statutes.

[1] *Best Practices: Elements of a Federal Privacy Program*, Federal CIO Council, (June, 2010), https://energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf.

Privacy Risk Management and Compliance Documentation

As a multifaceted operation, the State of Indiana requires a heightened level of awareness from its subject-matter experts to ensure that Government Information is maintained in a way that respects the privacy of individuals. The APO should have an understanding of current and forthcoming agency efforts that may involve the maintenance, management, or exchange of Government Information. The APO will ensure the inclusion of privacy principles and compliance where appropriate. In certain instances, a privacy impact assessment may be necessary. Such an assessment shall be completed in accordance with applicable IOT standards.[2]

The APO will oversee the annual submission of an information system report as required by Ind. Code. § 4-1-6-7. The information system report will be submitted using the mechanism prescribed by the IOT. The information system report will, at a minimum, include the following:

1) The name or descriptive title of the information system and its location.
2) The nature and purpose of the information system and the statutory or administrative authority for its establishment.
3) The categories of individuals on whom Personal Information is maintained, including the approximate number of all individuals on whom information is maintained and the categories of personal information generally maintained in the system, including identification of those which are stored in computer accessible records and those which are maintained manually.
4) All confidentiality requirements, specifically:
    (A) those information systems or parts thereof which are maintained on a confidential basis pursuant to a statute, contractual obligation, or rule; and
    (B) those information systems maintained on an unrestricted basis.
5) In the case of item (4)(A) above, the agency shall include detailed justification of the need for statutory or regulatory authority to maintain such information systems or parts thereof on a confidential basis.
6) The categories of sources of such Personal Information.
7) The agency's policies and practices regarding the implementation of Ind. Code § 4-1-6-2 relating to information storage, duration of retention of information, and elimination of information from the information system.
8) The uses made by the agency of Personal Information contained in the system.
9) The identity of agency personnel, other agencies, and persons or categories of persons to whom disclosures of personal information are made or to whom access to the system may be granted, together with the purposes therefor and the restriction, if any, on such disclosures and access, including any restrictions on redisclosure.
10) A listing identifying all forms used in the collection of personal information.
11) The name, title, business address, and telephone number of the person immediately responsible for bringing and keeping the system in compliance with the provisions of this chapter.

[2] Data Categorization (IOT-CS-SEC-105); Security Assessment and Authorization (IOT-CS-SEC-146); Collection and Storage of Personal Information (IOT-CS-SEC-103).

Information Security

Pursuant to Ind. Code Art. 4-13.1, the IOT has put forth the State of Indiana Information Security Framework, which provides requirements and direction to inform agency efforts relating to information security.[3] Pursuant to Ind. Code Ch. 5-15-5.1, the Indiana Archives and Records Administration ("ARA") has put forth records retention schedules, which govern the retention and disposition of governmental records.[4] Agencies are expected to be in compliance with both the IOT's Information Security Framework and the ARA's records retention schedules, as they may apply. In context of this Policy and in accordance with Ind. Code § 4-1-6-2, agencies must do the following:

1) Collect, maintain, and use only that Personal Information as is relevant and necessary to accomplish a statutory purpose of the agency.
2) Insofar as possible, segregate information of a confidential nature from that which is a disclosable public record and, pursuant to statutory authority, establish confidentiality requirements and appropriate access controls for all categories of Personal Information contained in the information system.
3) Maintain a list of all persons or organizations having regular access to Personal Information which is not a matter of disclosable public record in the information system.
4) Maintain a complete and accurate record of every access to Personal Information in a system which is not a matter of disclosable public record by any person or organization not having regular access authority.

Incident Response

State agencies are expected to comply with Ind. Code Ch. 4-1-11 and related policies put forth by the IOT. As applicable to state agencies, a breach is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a state or local agency. The term does not include the following:

1) Good faith acquisition of personal information by an agency or employee of the agency for purposes of the agency, if the personal information is not used or subject to further unauthorized disclosure.
2) Unauthorized acquisition of a portable electronic device on which personal information is stored if access to the device is protected by a password that has not been disclosed.

Ind. Code § 4-1-11-2.

If such an event occurs, the IOT maintains the Indiana Security Incident Response Team ("ISIRT"), which must be immediately alerted via isirt@iot.IN.gov. The ISIRT will respond and require state agency action in accordance with Information Security Framework Standards *IOT-CS-SEC-133* and *IOT-CS-SEC-134*.

Following the notification and any necessary remediation, the agency must provide to the CPO and ISIRT documentation of the mitigation, disclosure, and notification actions taken.

[3] https://secure.iot.in.gov/.
[4] http://www.in.gov/iara/2360.htm.

Notice and Redress for Individuals

A well-rounded privacy policy should provide for multiple independent verifications that the privacy of individuals is being maintained appropriately. It is on those lines that this Policy restates and reinforces that which the Indiana General Assembly has already put forth. Where a state agency maintains a system and holds title to the Government Information in the system, the agency must provide a mechanism for an individual to challenge, correct, or explain information in a system about the individual. Should a correction or explanation about the Government Information be added to the originating agency's system, that agency must notify other state agencies maintaining copies of the Government Information to ensure that all records are updated accordingly.

> Unless otherwise prohibited by law, any state agency that maintains a Personal Information system shall, upon request and proper identification of any data subject, or a data subject's authorized agent, grant the subject or agent the right to inspect and to receive at reasonable, standard charges for document search and duplication, in a form comprehensible to the subject or agent:
>
> (a) all Personal Information about the data subject, unless otherwise provided by statute, whether the information is a matter of public record or maintained on a confidential basis, except in the case of medical and psychological records, where the records shall, upon written authorization of the data subject, be given to a physician or psychologist designated by the data subject;
> (b) the nature and sources of the personal information, except where the confidentiality of the sources is required by statute; and
> (c) the names and addresses of any recipients, other than those with regular access authority, of Personal Information of a confidential nature about the data subject, and the date, nature, and purpose of the disclosure.

Ind. Code § 4-1-6-3.

> If the data subject gives notice that the data subject wishes to challenge, correct, or explain information about the data subject in the personal information system, the following minimum procedures shall be followed:
>
> (a) the agency maintaining the information system shall investigate and record the current status of that personal information;
>
> (b) if, after the investigation, the information is found to be incomplete, inaccurate, not pertinent, not timely or not necessary to be retained, it shall be promptly corrected or deleted;
>
> (c) if the investigation does not resolve the dispute, the data subject may file a statement of not more than two hundred (200) words setting forth the data subject's position;
>
> (d) whenever a statement of dispute is filed, the agency maintaining the data system shall supply any previous recipient with a copy of the statement and, in any subsequent

dissemination or use of the information in question, clearly mark that it is disputed and supply the statement of the data subject along with the information;

(e) the agency maintaining the information system shall clearly and conspicuously disclose to the data subject the data subject's rights to make a request;

(f) following any correction or deletion of personal information the agency shall, at the request of the data subject, furnish to past recipients notification delivered to their last known address that the item has been deleted or corrected and shall require the recipients to acknowledge receipt of the notification and furnish the data subject the names and last known addresses of all past recipients of the uncorrected or undeleted information.

Ind. Code § 4-1-6-5.

Privacy Awareness

While the State of Indiana's success in the maintenance of individual privacy begins with leadership, all state employees must be aware of and assist with privacy-focused efforts. All state employees should be familiar with this Policy and with the IOT's Information Security Framework. APOs are encouraged to educate employees of their agency regarding applicable privacy statutes and regulations.

Interagency coordination by and between APOs will assist in the State of Indiana's privacy compliance efforts. The CPO can assist APOs as they work to protect the confidentiality of individuals' information.

References

1. *Best Practices: Elements of a Federal Privacy Program*, Federal CIO Council, (June, 2010), https://energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf.

Revision History

Version	Date	Name	Revision Description
1	9/15/17	Ted Cotterill	Initial version.

Approval

Chief Data Officer
State of Indiana