

State of Ohio

Access Policies Resource Kit

Access Policies Working Group

March 8, 2010

Preface

This document was created as a result of the research conducted by the Access Policies working group under the Data Protection Subcommittee of the Multi-Agency CIO Advisory Council. Member agencies of the working group include:

Administrative Services

Medical Board

Taxation

Commerce

Natural Resources

Workers' Compensation

Health

Optical Dispensers Board

For more information, contact:

Office of Information Security & Privacy
Ohio Department of Administrative Services
30 East Broad Street, 40th Floor
Columbus, Ohio 43215

Telephone: 614-387-5682

Facsimile: 614-728-0837

E-mail: kevin.brown@oit.ohio.gov

These materials can also be found on the Internet at:
<http://www.privacy.ohio.gov/Government.aspx>

Overview

The purpose of this document is to assist state agencies in protecting the confidentiality of a specific category of data, in both electronic and paper forms, known as Confidential Personal Information (CPI). This document offers specific guidance in the following forms:

- An application model that agencies may use to determine the number and types of CPI access policies required by ORC 1347.15.
- Survey questions to assist agencies in gathering information on the organizational policies and procedures related to CPI access.
- Two case studies that illustrate use of the application model by state agencies.
- Information as to what constitutes misuse of CPI under Chapter 1347 of the Revised Code.

Agencies are encouraged to tailor these recommendations to meet their specific requirements.

Table of Contents

| | |
|---|----|
| Terms..... | 1 |
| Application Model for Accessing Confidential Personal Information..... | 4 |
| Survey Questions for the Development of Confidential Personal Information (CPI) Access Policies..... | 9 |
| Case Studies | |
| Applying Lessons Learned from Case Studies | 14 |
| Case Study #1: Ohio Medical Board | 15 |
| Case Study #2: Ohio Department of Commerce..... | 20 |
| Misuse of CPI..... | 43 |

Table of Figures

| | |
|---|----|
| Figure 1: User, Role and Identity Definition Relationships..... | 3 |
| Figure 2: Bottom-Up Method..... | 5 |
| Figure 3: Top-Down Method | 6 |
| Figure 4: System-Specific Method | 7 |
| Figure 5: Access Policy Documents | 8 |
| Figure 6: Commerce Access Policy Documents..... | 33 |
| Figure 7: Ohio Commerce Active Directory Structure..... | 40 |
| Figure 8: State Fire Marshal Active Directory Structure..... | 41 |

Terms

The following terms are used throughout this document:

Access - Ability to make use of any information system (IS) resource.

Confidential Personal Information (CPI) - Personal information that is not a public record for purposes of section 149.43 of the Revised Code.

Data classification - The process of determining the appropriate level of protection based on the confidentiality and criticality requirements of data in accordance with the agency's risk assessment per Ohio IT Policy ITP-B.1, "Information Security Framework."¹ Data classification implements policy-based standards for securing and handling data, and sharing information among organizations.

Data owners / stewards - Persons from a business or program area who are responsible for classifying data and generating guidelines for its lifecycle management. Some agencies use the term **data steward** to describe such individuals. As described in Ohio IT Policy ITP-B.11, "Data Classification," data ownership involves responsibility for the identification and classification of information, including such tasks as:

- Assign data classification labels;
- Provide that data is consistently classified after being compiled from multiple sources – summarizing information can often create or hide the presence of CPI;
- Coordinate data classification between agencies;
- Ensure that personally identifiable information is secured appropriately;
- Ensure that downloading data via remote access or to a portable computing device is performed appropriately; and
- Ensure that guidelines exist for accessing data and that these requirements can be incorporated into contractor service level agreements and contract terms and conditions.

Identity - The unique identifier for a user. A role is implemented through an identity.

Information system - A discrete set of electronic or paper information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Role - A construct that links job functions in an organization to the specific levels of access that users require to organizational resources. Roles are distinct from but related to position descriptions in that a role refers to the specific systems a user may access.

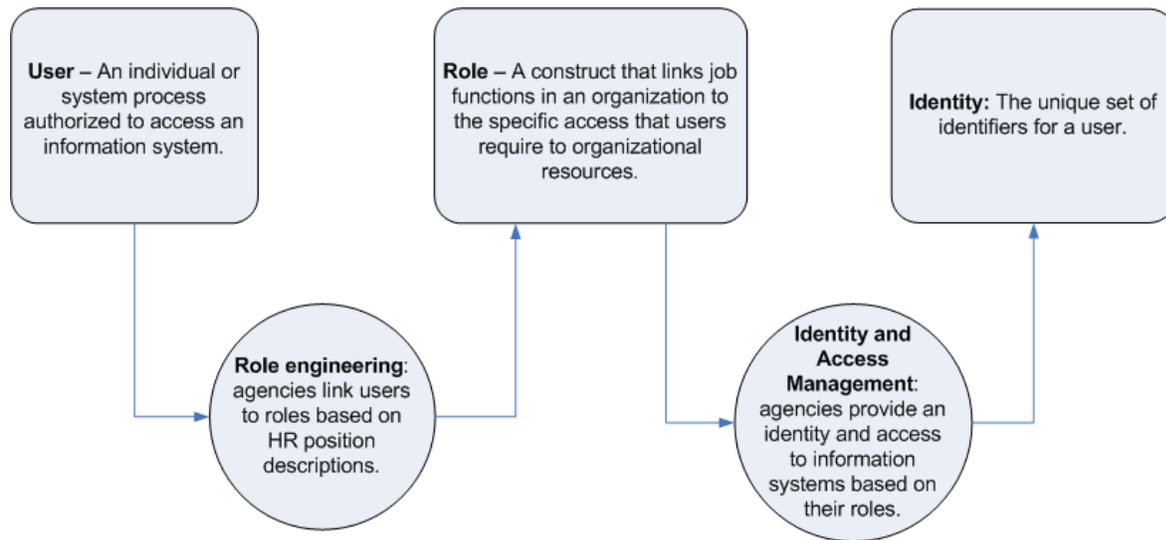
Role engineering - The process of defining roles.

System – "System" means any collection or group of related records that are kept in an organized manner and that are maintained by a state or local agency, and from which personal information is retrieved by the name of the person or by some identifying number, symbol, or other identifier assigned to the person. "System" includes both records that are manually stored and records that are stored using electronic data processing equipment. "System" does not include collected archival records in the custody of or administered under the authority of the Ohio historical society, published directories, reference materials or newsletters, or routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person.

User - An individual or system process authorized to access an information system. This access is typically based on the individual's role and is implemented through an identity.

¹All security- and privacy-related Ohio IT policies may be found at:
<http://privacy.ohio.gov/OhioPolicies.aspx>.

Figure 1: User, Role and Identity Definition Relationships



Application Model for Accessing Confidential Personal Information

Overview

Ohio Revised Code §1347.15 requires state agencies to adopt rules that regulate access to Confidential Personal Information (CPI). One such rule, as required by ORC §1347.15 (B)(2) shall include the following:

“A list of the valid reasons, directly related to the state agency's exercise of its powers or duties, for which only employees of the state agency may access confidential personal information;”

This portion of the statute requires state agencies to have clear statements describing **why** CPI access is permitted in the agency. Organizations typically document and communicate such statements to end-users in the form of access policies. The purpose of this application model is to provide a tool for agencies to develop such policies. Agencies should consider using this model once they have pursued a data discovery and classification effort, and have at least an initial sense of **where** CPI is maintained, and **who** will require access to it.

CPI access policies need not be lengthy documents, but at a minimum, such policies must:

- sufficiently notify agency employees of their responsibilities related to CPI,
- identify the basis or bases for which employees may access CPI, and
- clearly state the potential liabilities related to unauthorized CPI access.

How should an organization develop the appropriate access policies to ensure compliance with ORC 1347.15? The answer will vary depending on the structure of the organization and the types of data it maintains. An agency that maintains a very small amount of CPI may only need to develop one policy to capture all valid reasons for appropriate access. Multiple policies may be necessary if the agency has a wide variety of program areas and collects various forms of CPI.

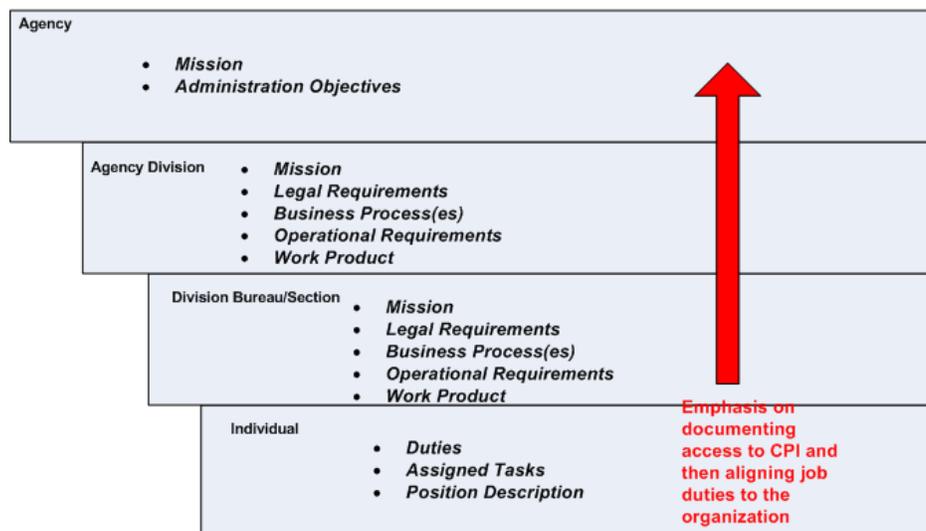
Application Model for Developing Access Policies

The application model described in this section may help data owners and data stewards to identify the number and types of access policies required by ORC 1347.15. Note that, due to the variety of environments within the state, organizations may need to further adapt one of these approaches:

A. The “Bottom-Up” Method:

The bottom-up approach to identifying “access drivers” begins with a review of individual employee activities involving CPI access, followed by a review of broader policies and business requirements at higher layers within the organization (See *Figure 2: Bottom-up Method* for an illustration):

Figure 2: Bottom-Up Method²



Individual functions are examined for alignment with agency mission and other organizational objectives. Where gaps on CPI access exist, the organization will likely develop guidance on CPI access at a procedural level, and ensure that these procedures align with broader agency or divisional policies. This method may be less appropriate for agencies with a large amount and variety of employees due to the amount of time necessary to review individual functions.

Bottom-up steps:

Step B-1. Agencies begin the policy development process through a review of employee duties, assigned tasks, and position descriptions. During this review, document wherever CPI access occurs and the reasons for such access. Any Privacy Impact Assessments that the agency has completed will help identify what systems contain CPI.

Step B-2. Upon completion of Step B-1, proceed to the next highest layer within the agency, for instance: a division, bureau, or program area layer. Ask the following questions for this layer:

- What is the mission of this layer?
- What legal or operational requirements within this layer require individuals to access CPI?
- What business processes within this layer require CPI?
- What systems support those business processes that require CPI?
- What work products involve CPI access during their development?

Document the responses to these questions and then repeat this step for each subsequently higher layer of the organization until the broadest agency-level statements have been identified.

² Note that this example implies that the agency is subdivided into divisions and bureaus. Smaller organizations may find their approach is “flatter” due to a fewer amount of layers.

Step B-3. Review the results of Steps B-1 and B-2, and, wherever possible, connect lower-level rationales for CPI access to higher-level objectives. For example:

Agency-level: ORC 4301.77: The division of liquor control may provide an SSN if the requesting agency is conducting an investigation, implementing an enforcement action, or collecting taxes.

Mid-level: Liquor Control Commission standard operating procedures guide employee steps for providing CPI to other state or local agencies.

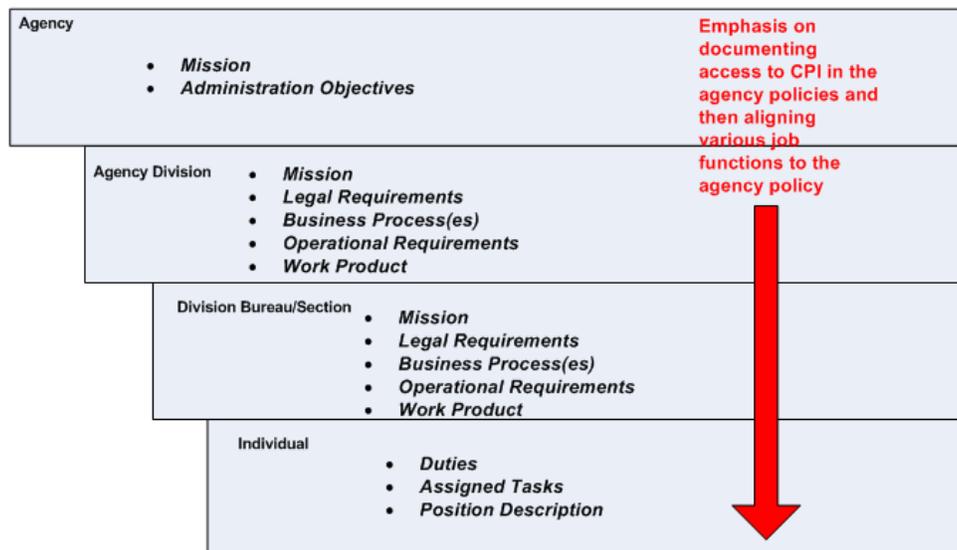
Individual access: Employee obtains social security number from Ohio's Liquor Law Enforcement Database to aid the investigator.

Ideally, every instance of an individual's access of CPI should ultimately trace up to higher-level, agency-wide mission and administration objectives. Wherever such access is not traceable, a gap may exist in CPI access policies.

B. The "Top-Down" Method:

The top-down approach begins with a review of agency mission and objectives, then proceeds down through the layers of an organization to ensure that lower-level policies and procedures align. This method emphasizes documenting CPI access at a policy-level. Larger agencies may find this method easier to leverage as the review of individual functions and position descriptions may be delegated to smaller units within the organization.

Figure 3: Top-Down Method³



Top-down steps:

Step T-1. Identify agency policy requirements that address access of CPI. If such policies do not exist, craft a high-level statement that addresses CPI access and tie that statement to the agency's mission and administration objectives.

³ Note that this example implies that the agency is subdivided into divisions and bureaus. Smaller organizations may find their approach is "flatter" due to a fewer amount of layers.

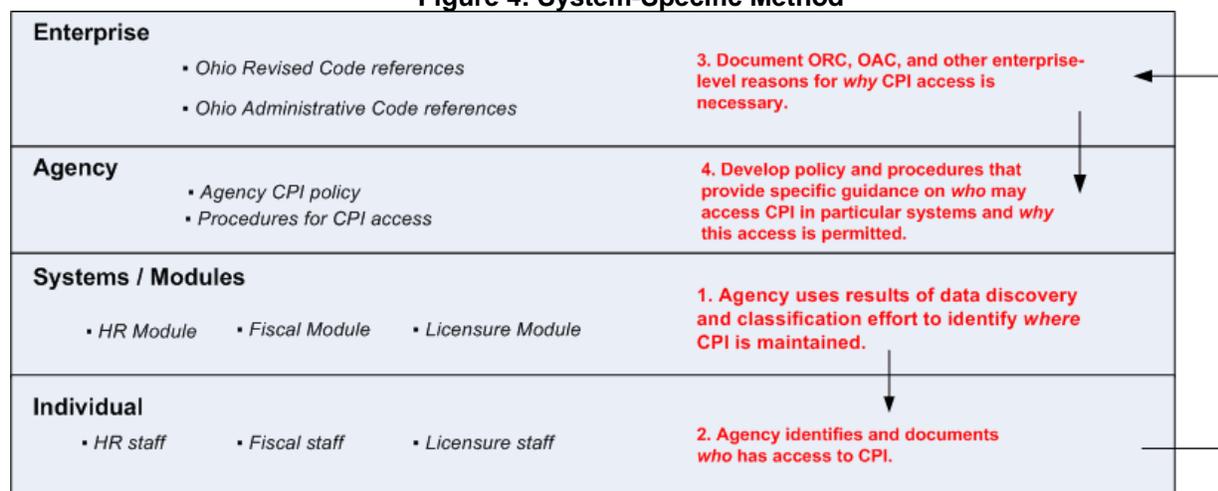
Step T-2. Review the mission requirements, business processes and work products for the next layer down within the organization (e.g., division, bureau or program area). Do policies or procedures at this layer adequately address both the responsibilities and liabilities associated with CPI access?

Step T-3. Develop or delegate development of CPI access policies and procedures based on the gaps identified in Step T-2. Ideally, every instance of an individual’s access of CPI should be traceable back to higher-level, agency-wide mission and administration objectives. Wherever such access is not traceable, a gap may exist in CPI access policies.

C. The System-Specific Method:

If an agency has completed a data discovery and classification effort that indicates where the agency maintains CPI, an alternate approach that leverages the results of this discovery process may be warranted. Agencies that already have a strong sense of where CPI is maintained within their environment may find this approach useful.

Figure 4: System-Specific Method



System steps:

Step S-1. Use the results of data discovery and classification to identify which information systems contain CPI.

Step S-2. Identify and document *who* has access to systems or system components containing CPI.

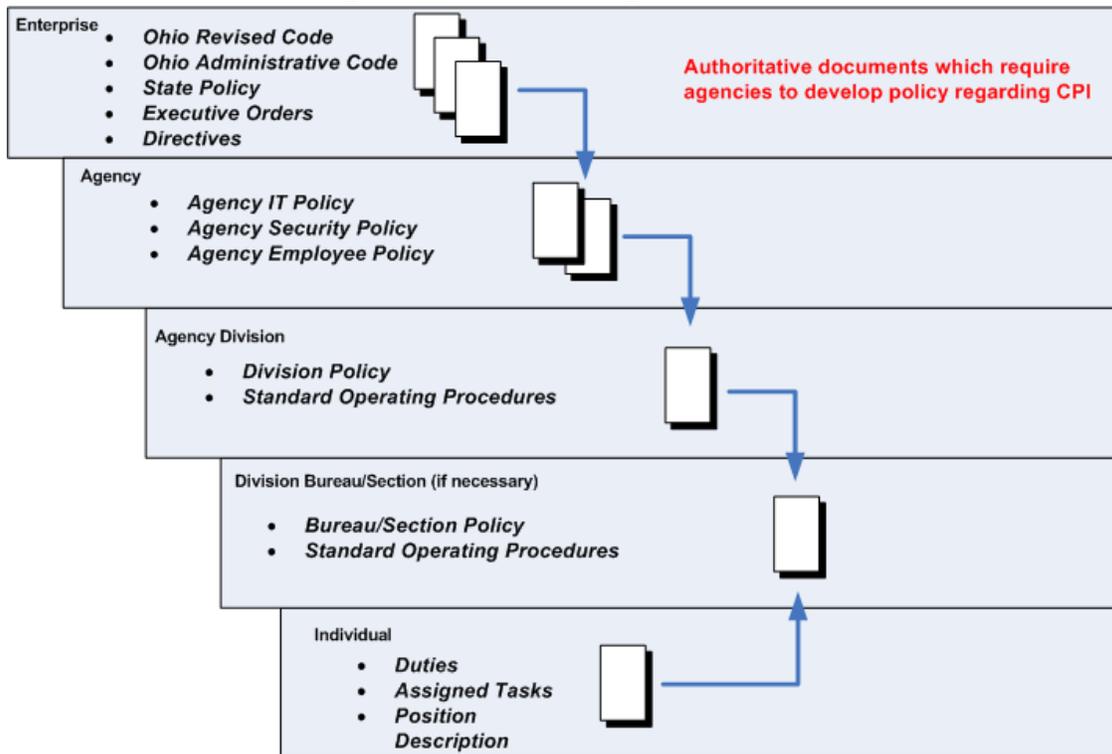
Step S-3. Review high-level policy documents that permit the agency to maintain CPI. Document *why* this access is necessary to perform agency functions.

Step S-4. Review the agencies policies and procedures related to CPI. Does this guidance adequately address both the responsibilities and liabilities associated with CPI access?

Access Policy Development Process:

Once an organization has completed a bottom-up, top-down or system-specific assessment and identified gaps in CPI access policies or procedures, it can begin development of new guidance to address these gaps. Figure 4 illustrates some potential forms of access documentation:

Figure 5: Access Policy Documents



Note that not all of these documents need to be in place to effectively address CPI access. Agencies should determine where CPI access is best addressed and ensure at a minimum that the policies:

- Notify employees of their responsibilities;
- reference the basis or bases for which agency employees may access CPI; and
- clearly state the potential liabilities related to unauthorized CPI access.

**Survey Questions for the Development of Confidential Personal Information (CPI)
Access Policies**

CPI Access Policies Assessment Tool

Agency Name:

General Instructions: Use this assessment tool to gather information on the organizational policies and procedures related to CPI access. Collect the following documents prior to the assessment to aid in the form's completion:

- mission statements
- administration objectives
- legal requirements
- operational requirements
- business process descriptions
- work product descriptions
- position descriptions
- descriptions of employee duties and tasks

1. Agency-Level Guidance

| | |
|---|--|
| a. What is the mission of the agency that requires CPI to be collected? | |
| b. What authority does the agency have to collect CPI? How would you describe this authority to people outside of the agency as well as the reason(s) the agency collects this information? | |
| c. Has the agency subjected its information collection requirements to rule review? | |
| d. Are there any organizational components of the agency exempt from ORC 1347? | |

| 1. Agency-Level Guidance | |
|---|--|
| e. Has the agency conducted any previous Privacy Impact Assessments (PIAs) or risk assessments? | |
| f. Has the agency established an internal standard format for its policies? | |

| 2. Division-Level Guidance | |
|---|--|
| a. What is the mission of the division that requires CPI to be collected? | |
| b. What authority does the division have in collecting CPI? | |
| c. What business processes within the division require CPI? | |
| d. What systems support those business processes that require CPI? | |
| e. What job functions or duties should have access to those supporting systems? | |

| 3. Bureau/Section Level Guidance | |
|---|--|
| a. What is the mission of the bureau/section that requires CPI to be collected? | |
| b. What authority does the bureau/section have in collecting CPI? | |
| c. What business processes within the bureau/section require CPI? | |

| 3. Bureau/Section Level Guidance | |
|---|--|
| d. What systems support those business processes that require CPI? | |
| e. What job functions or duties should have access to those supporting systems? | |

| 4 Job Function/Descriptions Level Guidance | |
|--|--|
| a. Why does the individual access CPI? | |
| b. Does the individual access CPI: <ul style="list-style-type: none">• as a result of research performed for official agency purposes,• routine office procedures, or• incidental contact? | |
| c. Is there a log that records specific access of CPI by this employee? | |
| d. Is the CPI access about an individual, and does the access occur as a result of a request by that individual for CPI about that individual? | |

CPI Access Authority Template

Agency Name:

General Instructions: Use this template to connect the results of a data discovery and classification effort to specific reasons for collecting and accessing CPI and to identify the current users with access to such CPI. See the agency case studies within this document for examples involving this template.

| Division/ Section OR Application/ Module | Records Description | Possible CPI | Confidential (If yes or limited, include citation) | Authority to Collect CPI | Access Authoriza tion | Reasons for access | Current Users/Access |
|--|------------------------|-----------------|--|--------------------------------|-----------------------------|-----------------------|-------------------------|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

CPI Access Policies Mapping

General Instructions: Agencies may use this mapping to summarize the results of the assessment tool in a concise manner.

| |
|---|
| Agency-level: <i>(may include Ohio Revised Code, Ohio Administrative Code, State Policy, Executive Orders, Directives)</i> |
| Mid-level: <i>(agency IT policies, agency security policies, agency employee policies)</i> |
| Individual-level: <i>(duties, assigned tasks, position, description)</i> |

Example Mapping:

| |
|---|
| Agency-level: ORC 121.08(D): There is hereby created in the department of commerce a division of liquor control, which shall have all powers and perform all duties vested by law in the superintendent of liquor control. Wherever powers are conferred or duties are imposed upon the superintendent of liquor control, those powers and duties shall be construed as vested in the division of liquor control. The division of liquor control shall be administered by the superintendent of liquor control. |
| Division-level: ORC 4391.77: The division of liquor control may provide the social security number of an individual that the division possesses to the department of public safety, the department of taxation, the office of the attorney general, or any other state or local law enforcement agency if the department, office, or other state or local law enforcement agency requests the social security number from the division to conduct an investigation, implement an enforcement action, or collect taxes. |
| Mid-level: The division of liquor control maintains security procedures related to an agency employee providing CPI to other state or local agencies. |
| Individual-level: Employee of the division of liquor control accesses a record, including CPI, of a liquor permit holder within the Ohio Liquor Law Enforcement Database for the purpose of assisting the Ohio Department of Public Safety with an investigation. |

Case Studies

Applying Lessons Learned from Case Studies

This section contains two case studies describing state agency approaches to CPI access policy development.

While both agencies pursued a similar approach, their results contain significant differences. The application model for developing access policies is highly flexible, and factors such as diversity in agency mission and the amount of CPI maintained by an agency can greatly affect the outcome of the process. Agencies reviewing these case studies for tips on their own efforts should keep these factors in mind:

- Diversity of mission – Agencies with fewer program areas will likely require fewer access policies. For example, a board or commission with a tightly focused mission may only require one CPI access policy. The Department of Commerce, though it only employs about 1,000 employees, nevertheless has a high number of access requirements due to the number of different activities housed within the agency (e.g., financial regulation, industrial compliance, State Fire Marshal, Unclaimed Funds and more).
- Agency organization – hierarchical organizations may have multiple layers of policies and procedures to reflect agency, division, bureau or section differences. “Flatter” organizations may have fewer, if any, layers between Revised Code, Administrative Code, and individual functions as described in this resource kit.
- Revised Code and Administrative Code – The degree of detail to which Revised Code or Administrative Code describes an agency’s mission may bear on CPI access policy development. Carefully review the agency’s authorizing statutes and related administrative rules as collecting CPI may be indirectly necessary to support a business function. Agencies that collect CPI and can find no high-level justification for it should carefully consider whether this collection should be eliminated.
- Amount of CPI/Uses for CPI – ORC 1347.15 addresses employee access of Confidential Personal Information. While those agencies that maintain little or no CPI may likewise spend less time on CPI access policy development, verify how business processes may use this information in different ways.

Case Study #1: Ohio Medical Board

Agency mission and description

The mission of the Ohio Medical Board is to protect and enhance the health and safety of the public through effective medical regulation. This mission is supported by the following goals:

- Ensure that those who are licensed by the Board meet certain minimum education and training criteria to safely practice medicine in Ohio.
- Rehabilitate, when possible, persons who are impaired or who practice medicine unethically or below minimal standards of care, and to prohibit persons who have not been rehabilitated from practicing medicine.
- Prohibit persons from practicing medicine whose violations are so egregious as to forfeit the privilege or who otherwise lack the legal authority.
- Provide information about the licensees of the Medical Board, the Board's functions and operations, and the laws governing the practice of medicine.
- Achieve and maintain the highest possible levels of organizational efficacy.

The Board consists of approximately 100 employees, including 12 board members. Licensee information collected and maintained by the Board is stored in an application called eLicensing, an electronic, indexed system that contains CPI. Active medical licenses maintained by the Board totaled approximately 60,000 in 2008. IT operations are supported by two full-time employees: a Data Administration Manager and a Network Administrator.

While the Board maintains highly confidential personal information that, in general, must be protected from unauthorized access, in certain instances, portions of this information can and should be shared with Ohio citizens for the public interest. Strong CPI access policies are therefore required to inform employees when they should access and provide access to CPI in a manner consistent with the agency's mission.

Use of the Application Model

Discovery of CPI

The Board initiated its ORC 1347.15 compliance effort by completing an assessment of all agency systems for CPI. CPI in the form of licensee information is primarily maintained in a system called "eLicensing"; thus the Board's "system review" evolved into a modular review of eLicensing.

SSNs are truncated in the display screen of eLicensing to protect users from accessing CPI on a regular basis. However, context is also important, and the Board is working to assess whether CPI access is possible through correlating different screens, links and reports generated in eLicensing.

An example of information collected by the Board's initial system review is shown in Table 1:

Table 1: Medical Board - CPI Access Worksheet

| Application / Module | Description | CPI Contained | Access Authorization | Who Accesses | Reasons for Access | Ref. Auth. For Confidentiality |
|-------------------------------|---|---------------------------|----------------------|--|--|--------------------------------|
| eLicensing Enforcement Module | Complaints database, attached documents | All Complaint information | Assistant Directors | All investigation, enforcement, compliance staff. IT staff, All Licensure & renewal staff have limited access. | Establish, investigate & resolve complaints; respond to status inquiry; verify status prior to license issuance; research legal concerns; IT maintenance | RC 4731.22(F)(5) |

Program areas and CPI

To fulfill the Board’s goals, the Board reviewed each of its five functional groupings to help determine why CPI access is necessary. This process, including the development of a CPI access policy, took about five half-day sessions (20 hours total) to complete.

The groupings include:

- License-oriented business
- Issues-related business
- Executive Staff
- Administration/Fiscal Office
- Hearing Unit

Below are brief descriptions of three of these Board groupings and an example of CPI that an employee in this program area may access:

License-oriented business- Validates educational and training credentials for licensure and renewal of licensure for all license types under the Board's jurisdiction. Prepares information for Medical Board review prior to issuance of license. Informs applicants of Board decisions. Example of CPI access: licensee registrations containing SSNs.

Issues-related business - Conducts field and office-based investigations of complaints alleging violations of the laws and regulations governing the practice of medicine and its branches in Ohio; gathers evidence relevant to the investigation, including by interview, surveillance, audit and review of prescription records, medical records, court records, etc.; monitors medical practitioners who are subject to a Board Order or consent agreement; provides information to assist the Board in making decisions concerning probationary requests and probationary status; and coordinates investigative activities with other entities, including law enforcement agencies. Example of CPI access: prescription records related to an investigation.

Executive Staff - Serves Executive Director; coordinates functions of other business program areas; answers non-routine inquiries; coordinates budget development; oversees Board Web presence; handles media relations. Example of CPI access: licensure information that contains an SSN related to a non-routine inquiry.

Legal authority and policy mappings

The enabling statute of the Medical Board is Ohio Revised Code §4731.01. Board authority is found throughout several chapters of the Revised Code⁴, as well as Chapter 4731 of the Administrative Code. The following mappings show the relationship between:

- the Board's powers and duties as described in ORC and OAC,
- program-level description for how these powers and duties are exercised, and
- examples of a Board employee's access of CPI for each program area.

Below each mapping is a draft policy statement potentially for use in a CPI access policy. Note how the statement:

- cites Ohio Revised Code or Ohio Administrative Code,
- provides context for a particular program area,
- is applicable to the example shown at the individual-level.

Mapping A: Collecting licensee data

| |
|---|
| Agency-level: ORC 4730.10: "(A) An individual seeking a certificate to practice as a physician assistant shall file with the state medical board a written application on a form prescribed and supplied by the board. The application shall include all of the following: (1) The applicant's name, residential address, business address, if any, and social security number;" |
| Program-level: <i>License-oriented business:</i> Validates educational and training credentials for licensure and renewal of licensure for all license types under the Board's jurisdiction. [Agency policies and procedures that address this program area are in draft.] |
| Individual-level: Board employee in the License-oriented business area enters an applicant's Confidential Personal Information into the eLicensing system. |
| Potential policy statement: Board employees may access CPI to process applications submitted in accordance with ORC 4730.10 that validate educational and training credentials for licensure and renewal of licensure for all license types. |

⁴ Ohio Revised Code 4730, 4731, 4760, 4762

Mapping B: Reviewing CPI for compliance

| |
|--|
| <p>Agency-level: OAC 4731-19-06: “(A) The board shall record a complaint and investigate to determine whether the licensee is infected with HIV or HBV; whether the licensee is likely to perform or participate in an invasive procedure; and whether there is evidence that the licensee has violated any provision of section 4730.25, 4731.22, 4760.13 or 4762.13 of the Revised Code.”</p> |
| <p>Program-level: <i>Issues-related business:</i> Monitors medical practitioners who are subject to a Board Order or consent agreement. Approximately 150 practitioners are on probation at any given time.</p> |
| <p>Individual-level: Medical Board compliance officer tracking confidential information re: HIV positive or Hepatitis B virus positive practitioners stored in eLicensing for compliance with Ohio Revised Code.</p> |
| <p><i>Potential policy statement:</i> In accordance with OAC 4731-19-06, Medical Board compliance officers may access CPI in the process of monitoring medical practitioners who are subject to a Board Order or consent agreement.</p> |

Mapping C: Reviewing complaints

| |
|--|
| <p>Agency-level: Ohio Revised Code 4731.22 (F)(1): “The board shall investigate evidence that appears to show that a person has violated any provision of this chapter or any rule adopted under it. Any person may report to the board in a signed writing any information that the person may have that appears to show a violation of any provision of this chapter or any rule adopted under it. [...] Each complaint or allegation of a violation received by the board shall be assigned a case number and shall be recorded by the board.”</p> |
| <p>Program-level: <i>Issues-related business:</i> Access CPI while processing complaints to establish, investigate and resolve complaints; respond to status inquiry; and verify status prior to license issuance.</p> |
| <p>Individual-level: Any of the Board’s investigation, enforcement and compliance staff may access CPI while processing a complaint.</p> |
| <p><i>Potential policy statements:</i> In accordance with ORC 4731.22(F)(1), Board staff may access CPI for the purposes of establishing, investigating, or resolving a complaint.</p> |

Mapping D: Administrative access

| |
|--|
| Agency-level: No statutes or administrative rules address administrative access of CPI, but one of the Board's goals does: "Achieve and maintain the highest possible levels of organizational efficacy." |
| Program-level: Administrative staff may help support any program area. |
| Individual-level: <i>Example A:</i> A Data Administration Manager accesses CPI in the process of troubleshooting an eLicensing reporting problem. <i>Example B:</i> A records manager accesses CPI while providing licensee information in support of one of the Board's program areas. |
| <i>Potential policy statements:</i> IT staff may require access to CPI while performing maintenance on Board information systems. Such access shall be limited to ensuring that Board information systems are operating efficiently and effectively. Records management staff may require access to CPI to support other program areas of the Board. This access shall be limited to ensuring that the Board's program areas can efficiently and effectively access information in support of legitimate goals. |

Mapping E: Non-routine inquiries

| |
|--|
| Agency-level: No statutes or administrative rules address non-routine inquiries, but one of the Board's goals does: "To provide information about the licensees of the Medical Board, the Board's functions and operations, and the laws governing the practice of medicine." |
| Program-level: <i>Executive staff:</i> answers non-routine inquiries. |
| Individual-level: Director or his or designee answers non-routine inquiry regarding a particular medical practitioner's case. |
| <i>Potential policy statement:</i> The Director of the Board or his or her designee may access CPI in the course of answering a non-routine inquiry. The reasons for: a) authorizing a Board employee to access this specific CPI and b) how such reasons directly relate to the state agency's exercise of its powers or duties must be documented. |

Next steps

The Board's next steps are to translate a spreadsheet document on CPI maintained by the Board and the reasons for CPI access into procedures.

Case Study #2: Ohio Department of Commerce

Case Study #2 is intended to show an approach made by a medium-sized and mission-diverse agency. While Case Study # 1 describes an agency with 100 or less employees that are engaged in a single regulatory mission, Case Study # 2 describes an agency that has ten times the employees and has many regulatory missions within an overarching agency organization. The agency chosen for this case study is the Ohio Department of Commerce.

Agency mission and description

The mission of the Ohio Department of Commerce is to safeguard the public while striving to regulate commerce in a reasonable, fair and efficient manner. This mission statement is broad in nature because it must be applied to nine (9) separate divisions within the agency. Each agency division has a different mission. Within each of the divisions there are distinct bureaus which may have several different goals and objectives. Several boards or commissions also reside inside some of the agency's divisions. The various divisions, their bureaus and boards include:

- Division of Administration – provides overall administrative support for the agency and consists of a senior management team; a legal section; a legislative section; a communications section; an information technology group; a human resources, training, and labor relations section; and a support services section. In addition, the Division of Administration houses the Video Service Regulation Group which administers and enforces Ohio's video service authorization laws.
- Division of Financial Institutions – regulates Ohio's state-chartered depository institutions (banks, credit unions, savings banks, savings and loan associations) and non-depository financial service providers. The Division also regulates trust companies and licenses domestic and foreign money transmitters. Examination, supervision, and regulatory activities are performed by Division staff specializing in the operations of each specific financial industry. The Division is responsible for licensing pawn brokers, mortgage brokers, loan officers, credit service organizations, check cashing services, precious metal dealers, premium finance companies, and second mortgage lenders. The Division's Office of Consumer affairs educates Ohioans on how to protect themselves in the mortgage lending process, receives complaints against lenders, and refers borrowers to other organizations that can assist them. Enforcement actions are initiated when lending laws have been violated and cases are referred to prosecution.
- Division of Industrial Compliance – provides regulatory certification and inspections of boiler and elevator systems within the State. The division also conducts inspections of plumbing, electrical and structural systems, as well as bedding and upholstered products. The division reviews and approves building plans for the construction and renovation of commercial and public buildings and provides testing, certification, licensing and continuing education for numerous skilled trades in Ohio's building industry. The Division also inspects Ohio's ski tramways and historical boilers, and registers Ohio's roller rinks.
- Division of Labor & Worker Safety - administers and enforces Ohio's prevailing wage, minimum wage, overtime, and minor labor laws. The division's field staff conducts statewide inspections of workplaces for potential minor wage law violations. The Division of Labor and Worker Safety also educates employers and employees about their rights and responsibilities in the workplace.

- Division of Liquor Control – is responsible for controlling the manufacture, distribution, and sale of all alcoholic beverages in Ohio. The Division is the State’s sole purchaser and distributor of spirituous liquor, sold through more than 440 private businesses which contract with the Division to serve as its sales agents. Regulatory functions include the issuance of permits to the State’s approximately 24,000 privately owned and operated manufacturers, distributors, and retailers of alcoholic beverages. Besides spirituous liquor, the Division also regulates industry compliance with the laws pertaining to the manufacture, importation, and distribution of beer, wine, and mixed beverages.
- Division of Real Estate & Professional Licensing - The Division is responsible for licensing Ohio's real estate brokers and salespeople, real estate appraisers, and foreign real estate dealers and salespeople. The Division is also responsible for the registration of cemeteries located in Ohio and the registration of real estate developments located in other states but marketed in Ohio.
- Division of Securities – attempts to maintain a balance between enhancing capital formation and providing investor protection by administering and enforcing the Ohio Securities Act. The Act requires the licensing of those who sell securities or give advice about investing in securities; provides for the registration or exemption of securities sold; and prohibits certain conduct with the sale of securities and the giving of advice about investing in securities.
- State Fire Marshal (SFM) – This Division’s activities focus on education, research, regulation, and enforcement in the area of fire safety and fire prevention. Ohio's Division of State Fire Marshal, located in Reynoldsburg, is the oldest established office of its kind in the United States. SFM consists of eight bureaus: Administration, Bureau of Underground Storage Tank Regulation (BUSTR), Code Enforcement, Fire Prevention, Forensic Laboratory, Investigation Bureau, Ohio Fire Academy, and Testing and Registration. The Administration section provides administrative, communications, fiscal, and legal support for the SFM's Office. It also organizes special events such as the Ohio Fire Service Hall of Fame ceremony. The Fire & Explosion Investigation Bureau investigates fires and explosions throughout Ohio and is basically a functioning police department engaged in conducting felony investigations. The Forensic Laboratory analyzes evidence from fires and explosions as well as hazardous material leaks and spills. BUSTR regulates and enforces Ohio's underground storage tank regulations. The Fire Prevention Bureau educates Ohio's citizens about preventing fires and promotes good fire and life safety practices for individuals, schools, homes, and businesses. The Code Enforcement Bureau inspects hotels, motels, hospitals, and other buildings to ensure that they are up to the standards set by the Ohio Fire Code. The Ohio Fire Academy provides training to firefighters and emergency responders through diverse, accredited courses on campus and through the Direct Delivery Program. The Testing & Registration Bureau oversees the regulatory responsibilities of the companies and individuals licensed and regulated by the Division of State Fire Marshal.

The SFM's Office has worked extensively in the areas of Incident Command and Management, Weapons of Mass Destruction training, and personnel protection equipment for all of Ohio's first responders, including fire, EMS, law enforcement, health, and public works.

The SFM also is responsible for modernizing, promulgating and enforcing the Ohio Fire Code; designing and presenting fire prevention programs; analyzing fire-related

criminal evidence; investigating the cause and origin of fires and explosions; training firefighters; providing fire safety education to business, industry and the general public; regulating underground storage tanks; testing and training; and licensing and certification support services.

- Division of Unclaimed Funds – is responsible for safekeeping and returning money designated as “unclaimed.” The division has more than 4,500,000 accounts worth approximately \$1,200,000,000 in its custody.

Operational boards and commissions within the various divisions include:

Division of Financial Institutions

The Banking Commission, the Credit Union Council, and the Savings and Loan Associations & Savings Bank Board are associated with this division. All act in an advisory manner.

Division of Industrial Compliance

The Board of Building Appeals - reviews appeals made to adjudication orders issued by the Division of Industrial Compliance’s bureaus of Building Code Compliance and Operations & Maintenance or any certified local county enforcement agency. The Board also reviews appeals made to fire citations issued by the State Fire Marshal or any local fire department with a certified fire safety inspector.

The Board of Building Standards - formulates and adopts rules governing the Ohio Building Code. The Board also certifies municipal corporations, county, and township building departments to enforce the Ohio Building Code.

The Ohio Construction Industry Licensing Board - issues licenses to qualified electrical; heating, ventilating and air conditioning (HVAC); and plumbing, hydronics and refrigeration contractors who successfully pass the International Code Council licensing examination.

The Ohio Historical Boiler Licensing Board – oversees the testing, licensing and inspection of historic boiler operators and equipment.

The Ski Tramway Board – oversees the registration and inspection of ski/tram systems in the State.

Acting in an advisory capacity are the Electrical Safety Inspector Advisory Committee and the Residential Construction Advisory Committee.

Division of Liquor Control

Liquor Control Commission (LCC) – The LCC is independent from Commerce at this time, though the Department funds the LCC and is increasingly a custodian of its stored data.

Real Estate & Professional Licensing

The Ohio Real Estate Commission – reviews hearing examiner reports each month regarding real estate license law violations and its consideration of license appeals on licensure issues. To enforce the law, the Commission can revoke or suspend a license, assess a fine or order

additional continuing education. The Commission also hears cases against persons without a license performing activities that require a license.

The Real Estate Appraiser Board – oversees the operation of Ohio's real estate appraiser licensure and certification program. To enforce the law, the Board can revoke or suspend a license or certification, assess a fine or order additional continuing education.

The Cemetery Dispute Resolution Commission – assists in resolving complaints against registered cemeteries.

State Fire Marshal

The State Fire Commission – conducts research and publishes reports on fire safety and makes recommendations to the Governor, General Assembly, and other state agencies on any needed changes in laws, rules or administrative policy relating to fire safety.

The Petroleum Underground Storage Tank Release Compensation Board – administers the Ohio Financial Assurance Fund, created in response to federal regulations mandating that all owners and operators of petroleum underground storage tanks demonstrate the financial ability to pay for potential damages caused by releases from the tanks.

Use of the Application Model

Discovery of CPI

With such diversity in regulatory mission, a thorough review of how and where CPI is collected within the Department of Commerce was required to protect those involved in the regulatory processes. Strong CPI access policies are required both to inform employees when they should access and provide access to CPI in a manner consistent with the agency's mission and to protect those being regulated.

The Agency initiated its ORC 1347.15 compliance effort by completing an assessment of all agency systems for CPI. Unlike Case Study #1, where CPI was primarily licensee information contained in one system called "eLicensing," the Department of Commerce has more than 60 applications supporting its various missions. The variety of agency operations combined with the hundreds of agency forms, numerous applications, databases, and file or hardcopy repositories called for a bureau-by-bureau assessment that would also identify common types of CPI as well as CPI specific to each division, bureau, or board and commission. To accomplish the assessment, Commerce implemented the following process:

- 1) The agency's legal team, which reports to the Division of Administration but has attorneys assigned to each division, first met with Commerce's Information Technology Group to understand the impact of House Bill 648 and other aspects of ORC 1347.15.
- 2) Once understood, the legal staff crafted a Microsoft Excel spreadsheet to catalogue CPI. The spreadsheet has a separate worksheet tab for each division and bureau and a "general" worksheet tab for CPI identified as common across the agency.
- 3) The legal staff then conducted a thorough review of each division's legal requirements with regard to public information laws (ORC 149.43), its mission requirements for collecting CPI, and ORC 1347.15. Case law was also reviewed.

- 4) As the legal review progressed, the spreadsheet was updated and compiled.
- 5) The spreadsheet will be used for the following purposes:
 - a. To develop agency-level access policies, division-level access policies and even specific bureau-level policies using the “top down model” described elsewhere in this resource kit.
 - b. To develop the appropriate rules governing agency, division, and bureau handling of CPI.
 - c. To identify which bureaus may be exempt from 1347.15.
 - d. As a reference to regulatory reform processes as put forth in Executive Order 2008-04S, “Implementing Common Sense Business Regulation.”
 - e. In conjunction with data classification efforts as put forth in Ohio IT Policy ITP-B.11, “Data Classification”; in the Governor’s Management Directive of November 20, 2008 (revised April 2009); and in DAS-OIT Bulletins.

Commerce CPI Access Spreadsheet Examples

Several examples from the Department of Commerce CPI spreadsheet are shown over the next few pages. From the Division of Financial Institutions, here is one line from a 45-line spreadsheet:

Table 2: Commerce, Division of Financial Institutions - CPI Access Worksheet

| Division /Section | Records | Authority to Collect | Confidential | Cite | Possible Confidential Personal Information | Medium | Current Users Access |
|--|--|----------------------|--------------|-------------|---|--|--|
| DFI - Banks, Savings Institutions (BSI) | Banks - examination reports, work papers and exam related correspondence | ORC 1121.10; 1121.11 | Yes | ORC 1121.18 | Customer Information, which may include social security and taxpayer ID numbers, address, phone and electronic contact information, account numbers and other account, financial, health, family and business information Business information, including assets, net worth, liabilities, audit reports, financial reports, strategic business plans and budgets, and other related information. | Paper, disc, electronic systems (hard drive, H drive, shared drives, DFI-CIS, Intellivue), and microfilm | (1) Superintendent (2) BSI Deputy Superintendent (3) Superintendent's AA (4) BSI Examiners (5) BSI Support Staff (6) BSI Corporate Activities Staff (7) BSI Attorney Examiners (8) Division Counsel (9) Division Records Personnel |

From the Division of Industrial Compliance, here are several lines from a 60 line spreadsheet:

Table 3: Commerce, Division of Industrial Compliance - CPI Access Worksheet

| DIC SECTION/BOARD | Department Identified Confidential Personal Information (CPI) as defined by RC 1347.15 kept by the Division | Citation | Form CPI Kept | Record Kept containing CPI | Division-Specific CPI not on Department List? | Citation |
|-------------------|---|---|----------------------------|--|---|----------|
| Administration | Employee Home Address | State ex rel. Dispatch Printing Co. v. Johnson, 106 Ohio St. 3d 160, 2005 Ohio 4384, at ¶39 | Email, paper, network docs | Personnel file, employee contact list | No | NA |
| | Employee Personal Phone | State ex rel. Dispatch Printing Co. v. Johnson, 106 Ohio St. 3d 160, 2005 Ohio 4384, at ¶39 | Email, paper, network docs | Personnel file, employee contact list | | |
| | Employee personal email | State ex rel. Dispatch Printing Co. v. Johnson, 106 Ohio St. 3d 160, 2005 Ohio 4384, at ¶39 | Email, paper, network docs | Personnel file, employee contact list | | |
| | Employee SS# | 5 USC 522a; R.C. 149.43(A)(1)(v); State ex rel. Office of Montgomery County Pub. Defender v. Siroki, 108 Ohio St. 3d 207, 2006-Ohio-662, at 17-18; State ex rel. Beacon Journal Publishing Co. v. Akron (1994), 70 Ohio St.3d 605, 610, 1994-Ohio-6 | Email, paper, network docs | Personnel file | | |
| | Employee Medial Records | R.C. 149.43(A)(1)(a) | Email, paper, network docs | Personnel file | | |
| | Employee Bank Acct # | State ex rel. Beacon Journal Publishing Co. v. Akron (1994), 70 Ohio St.3d 605, 610, 1994-Ohio-6; State ex rel. Dispatch Printing Co. v. Johnson, 106 Ohio St. 3d 160, 2005 Ohio 4384, at ¶39. | Email, paper, network docs | Personnel file (copy of personal check for direct deposit) | | |
| | Accurint (if CPI occur in document) | | Outside Database (1 user) | NA | | |

From the Division of Real Estate & Professional Licensing, here are several lines from a 65 line spreadsheet:

Table 4: Commerce, Division of Industrial Compliance - CPI Access Worksheet

| Section | Authority to Collect Data | Types of "Confidential" Data Collected | CPI? (using line # from General tab) | CPI not on General List? | Authority that makes this Division specific CPI "confidential" |
|-----------|--|--|--------------------------------------|--------------------------|--|
| Legal/Enf | R.C. 4763.03(B); 476311.(G); R.C. 4735.05(B)(2) | CAVU Enforcement Case Data | 39 | No | <i>R.C. 4735.05(D); R.C. 4763.03(D)</i> |
| | R.C. 4763.03(B); 476311.(G); R.C. 4735.05(B)(2) | Intelliview- Enforcement/Legal | 39 | No | <i>R.C. 4735.05(D); R.C. 4763.03(D)</i> |
| | R.C. 4763.03(B); 476311.(G); R.C. 4735.05(B)(2) | Microfiche-Enforcement/Legal | 39 | No | <i>R.C. 4735.05(D); R.C. 4763.03(D)</i> |
| | R.C. 4735.25 | Foreign Real Estate Applications- Financial Records and Account Numbers | 19, 15 | No | |
| | R.C. 4763.03(B); 476311.(G); | Appraiser Disciplinary Case Files | 39 | | <i>R.C. 4735.05(D); R.C. 4763.03(D)</i> |
| | | Confidential – work product or information received during investigation | 39 | Yes | |

From the Division of Securities, here are several lines from a 65 line spreadsheet:

Table 5: Commerce, Division of Securities - CPI Access Worksheet

| Division of Securities/Section | Authority to Collect Data | Types of "Confidential" Data Collected | CPI? (using line # from General tab) | CPI not on General List? | Authority that makes this Division specific CPI "confidential" |
|-------------------------------------|--|--|--|--------------------------------------|---|
| Enforcement | Investigates violations of the Ohio Securities Act, Ch. 1707, pursuant to 1707.23 and 1707.36. Violations of 1707.44 are felonies. | The office of the Attorney-Inspector is designated a criminal justice agency (1707.36(A)). RC 1347.04(A)(1)(a) exempts from the chapter any state agency, or part...that performs as its principal function any activity relating to the enforcement of the criminal laws. Violations of 1707.44 are felonies. | exempt from CPI | | Background information and other data that would be CPI not included because would be gathered pursuant to criminal justice agency exemption. |
| Registration and Control Bid | 1707.03, 1707.041, 1707.06, 1707.09, 1707.091 | Registration primarily maintains records that are open to public inspection (1707.12). The only exceptions are the offering materials filed with exempt transactions under divisions (Q) and (W) of 1707.03 (see 1707.12(A)). | Not for Forms. It is unlikely that there will be CPI in the offering material since it is distributed outside of government. | Potentially trade secrets, line # 20 | No information in forms Q or W constitutes CPI, although 1707.12(A) provides the offering materials filed with the forms are confidential. |
| Licensing | Licenses securities dealers, salespersons, investment advisors, investment advisor representatives, state retirement system investment officers and bureau of workers' compensation chief investment officer pursuant to 1707.14, 1707.141, 1707.15, 1707.151, 1707.16, 1707.161, 1707.162, 1707.163, 1707.164, 1707.165, 1707.17, 1707.18 | SS#, fingerprint results, examinations, internal notes, client records, criminal investigative information | 7, 8, 16?, 17, 18, 19, 20, (25-31 are also exempt under law enforcement), 26, 30, 31, 36, 37, 38, 39 | | 1707.12(B) any investigative records non-public. This includes licensing investigations. |

And finally an example from the Division of Unclaimed Funds:

Table 6: Commerce, Division of Unclaimed Funds - CPI Access Worksheet

| Data | CPI | CPI Reasoning | Data Location | Types of Documents | Authority to Collect, Access Data |
|-----------------------------------|-----|---|--|--|---|
| Social Security Numbers | Yes | | Wagers Intellivue Flat files Accurint Microfiche | Claim forms Holder reports Paid claim files Death certificates, life insurance, other proof of ownership docs | RC 169.06, 169.08, OAC 1301:10-4-01 and 1301:10-4-02. |
| Federal Tax Identification | No | Public record under RC 149.43. | Wagers Intellivue Flat files Microfiche Accurint | Claim forms Holder reports Paid claim files Proof of ownership docs | RC 169.01; 169.02; 169.03; 169.05, 169.06, 169.08, OAC Chapters 1301:10-3 and 1301:10-4 |
| Financial account numbers | Yes | Although Public record under the public records law. No exception under RC 149.43. | Wagers Intellivue Microfiche | Claim forms, holder records, proof documents submitted by claimant. | RC 169.01; 169.02; 169.03, 169.05; 169.06; 169.08 |
| Wagers UPS 2000 | Yes | Property, claim and holder report information contain SSNs and financial account numbers. | Wagers | | RC 169.01, 169.02, 169.03 |

| Data | CPI | CPI Reasoning | Data Location | Types of Documents | Authority to Collect, Access Data |
|--|-----|--|--|--|--|
| Correspondence to holders | No | Except for audit records, public record under ORC 169.03(F)(4); 169.03(F)(3)(a) and OAC 1301:10-3-04(B) and (H). | Flat files, e-mail | | RC 169.01, 169.02, 169.03; 169.05, OAC Chapter 1301:10-3-03. |
| Claims correspondence | No | Public record under ORC Chapter 149. | Wagers, flat files, e-mail Intellivue | | RC 169.08; OAC Chapter 1301:10-4. |
| Holder audit/examination records, work papers | Yes | Audit records confidential under ORC 169.03(F)(4); 169.03(F)(3)(a) and OAC 1301:10-3-04(B) and (H). | Hard copies | | RC 169.01; 169.02; 169.03; 169.05; 169.10; 169.11; 169.12; 169.99; OAC Chapter 1301:10-3 |
| Paid claim files | No | Contains social security numbers, federal tax ID, financial account numbers of closed accounts, driver's license or other personal ID. | Wagers, Intellivue | Claim form, death certificates, life insurance, other proof documents submitted with claims. | RC 169.08; OAC Chapter 1301:10-4. |
| Claim records submitted by claimant | No | Contains social security numbers, federal tax ID, financial account numbers of closed accounts, driver's license or other personal identification. | Wagers, Intellivue | Death certificates, life insurance policies, other personal proof documents submitted with claims. | RC 169.08; OAC Chapter 1301:10-4. |
| Driver's license or identification card | No | Could contain SSN. | Intellivue | | RC 169.08; OAC Chapter 1301:10-4. |

Legal & Administration

| | | | | | |
|---|-----|--|------------|--|--|
| Legal Monthly and Weekly reports | Yes | | Flat files | | |
|---|-----|--|------------|--|--|

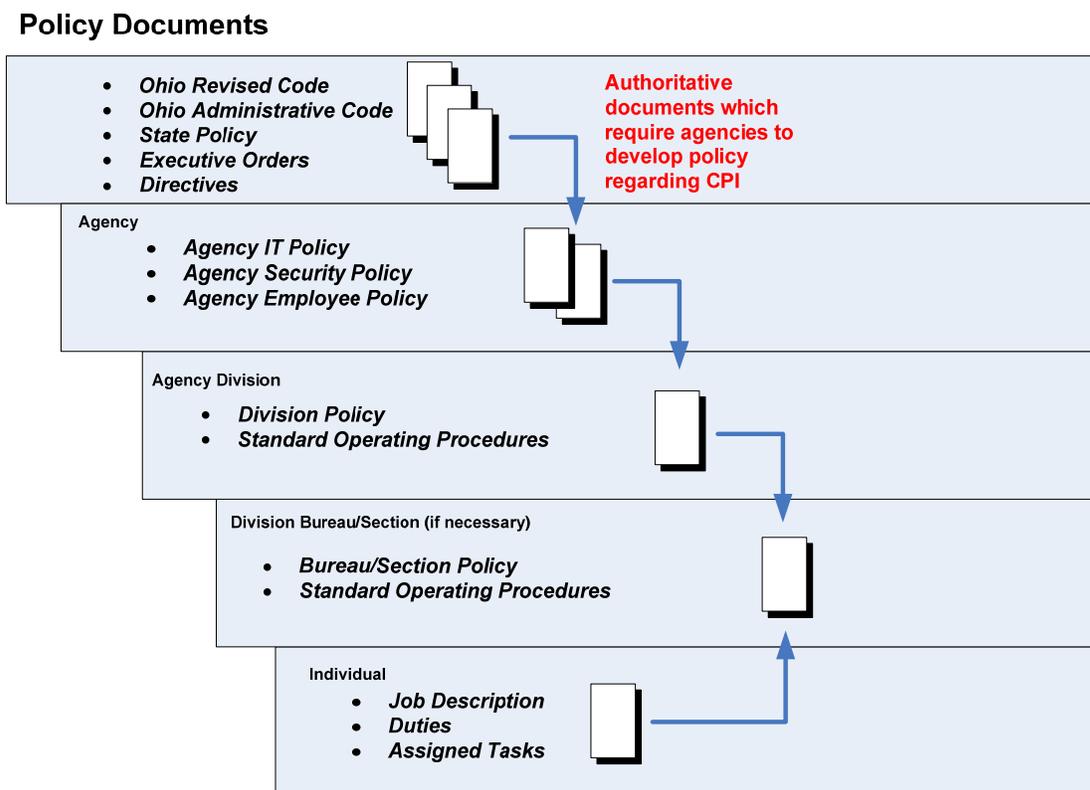
| Data | CPI | CPI Reasoning | Data Location | Types of Documents | Authority to Collect, Access Data |
|--|------------|----------------------|----------------------|---------------------------|---|
| Superintendent's Weekly Reports | May be | Public record? | Flat files | | |
| Claims policies | No | Public record | Flat files | | |
| Claims manual | No | Public record | Flat files | | |
| Vendor Contracts | No | Public record | Flat files | | |
| Executive correspondence | No | Public record | Flat files | | |
| General correspondence | No | Public record | Flat files | | |
| Routine correspondence | No | Public record | Flat files | | |
| Pleadings | No | Public record | Flat files | | |
| Attorney Work Product | Yes | | | | |
| Attorney-client communications | Yes | | | | |
| Consumer complaint | No | Public record | | | |
| Finder application | No | Public record | Locked file | | RC 169.13; 169.14; 169.16; 169.17; 169.99 |
| Licenses, certifications | No | Public record | Locked file | | RC 169.13; 169.14; 169.16; 169.17; 169.99 |

| Data | CPI | CPI Reasoning | Data Location | Types of Documents | Authority to Collect, Access Data |
|--|-----|---|----------------------------|--------------------|---|
| Criminal background checks- finder applicants | Yes | 42 USC 3789g, 28 CFR 20.21, 20.33A, R.C. 109.57(D) & (E), OAC 109:05-1-01, 4501:2-10-06 | Hard copies in locked file | | RC 169.13; 169.14; 169.16; 169.17; 169.99 |
| RC 119 Notices | No | Public record | Flat files | | RC 169.08; 169.09; 169.17 |
| CD Rom of Accounts (finders) | No | Public record, but contains financial account numbers | Wagers | | RC 169.06; 169.08; OAC Chapter 1301:10-4. |

Program Areas, CPI, and Policy Creation

To develop agency-level access policies, division-level access policies and even specific bureau-level policies, the spreadsheets were used to determine which parts of the Department’s organization were exempt; which areas could be covered by an overarching enterprise policy; and which required specific policies that were in line with their specific missions. Using the “top down model” described more thoroughly elsewhere in this resource kit, the Legal and IT teams at Commerce would develop a number of policy documents for each organizational level: agency, division, and bureau or section. Basically, this amounts to a tiered policy approach.

Figure 6: Commerce Access Policy Documents



Because Commerce has more than 800 employees, “hard coding” CPI access roles and rights into each and every job description or position description would be cumbersome and not very flexible. Using the “top down” model, various job descriptions can be referenced in each of the bureau or section level policies. Whole groups of individuals can then be covered in one policy document.

Development of CPI access policies: Mapping

To illustrate the creation of tiered policy and the mapping of its development, the Division of State Fire Marshal and four of its eight bureaus will be shown using the top down model. Each mapping example will have a different outcome reflected in the potential policy statement.

Mapping A: Department of Commerce; State Fire Marshal; Bureau of Underground Storage Tank Regulation (BUSTR)

Agency-level: ORC 121.02; 121.03; 121.04; 121.07; and 121.08; which establishes the Ohio Department of Commerce, its various divisions and their missions. ORC 1347.15 which defines how agencies must handle CPI and ORC 149.43 which defines how agencies must maintain public records.

Division-level: 3737.88 (A)(1) The fire marshal shall have responsibility for implementation of the underground storage tank program and corrective action program for releases from underground petroleum storage tanks established by the "Resource Conservation and Recovery Act of 1976," 90 Stat. 2795, 42 U.S.C.A. 6901, as amended. To implement the program, the fire marshal may adopt, amend, and rescind such rules, conduct such inspections, require annual registration of underground storage tanks, issue such citations and orders to enforce those rules, enter into environmental covenants in accordance with sections 5301.80 to 5301.92 of the Revised Code, and perform such other duties, as are consistent with those programs. The fire marshal, by rule, may delegate the authority to conduct inspections of underground storage tanks to certified fire safety inspectors.

(A)(2) In the place of any rules regarding release containment and release detection for underground storage tanks adopted under division (A)(1) of this section, the fire marshal, by rule, shall designate areas as being sensitive for the protection of human health and the environment and adopt alternative rules regarding release containment and release detection methods for new and upgraded underground storage tank systems located in those areas.

3737.88 (D) For the purpose of sections 3737.87 to 3737.89 of the Revised Code, the fire marshal shall adopt, and may amend and rescind, rules identifying or listing hazardous substances.

Bureau-level: 1. In accordance with 42 USC § 6991a [RCRA], administering and enforcing the licensure, environmental and fire safety provisions of R.C. §§ 3737.88, 3737.88.1, 3737.88.2, 3737.89, 3737.99(H) & (I).

2. In accordance with 42 USC § 6991a [RCRA] administering, developing and enforcing the Underground Storage Tank code promulgated in accordance with R.C §§ 3737.87, 3737.88, 3737.881, 3737.882 and 3737.89.

Potential policy statement: Only those employees assigned to the Bureau of Underground Storage Tank Regulation and engaged in processes, activities, and work duties associated with the bureau may access CPI of the bureau. BUSTR employees may access CPI to process documents submitted in accordance with ORC 3737.87; 3737.88; and 3737.89. All other access related to CPI within the agency or division shall be denied.

Mapping B: Department of Commerce; State Fire Marshal; Code Enforcement Bureau

Agency-level: ORC 121.02; 121.03; 121.04; 121.07; and 121.08; which establishes the Ohio Department of Commerce, its various divisions and their missions. ORC 1347.15 which defines how agencies must handle CPI and ORC 149.43 which defines how agencies must maintain public records.

Division-level: 3737.22(A) The fire marshal shall do all of the following:

- (1) Adopt the state fire code under sections 3737.82 to 3737.86 of the Revised Code;
- (2) Enforce the state fire code;
- (10) Conduct licensing examinations, and issue permits, licenses, and certificates, as authorized by the Revised Code;
- (11) Conduct tests of fire protection systems and devices, and fire fighting equipment to determine compliance with the state fire code, unless a building is insured against the hazard of fire, in which case such tests may be performed by the company insuring the building;
- (12) Establish and collect fees for conducting licensing examinations and for issuing permits, licenses, and certificates;

3737.22 (D)(1) The fire marshal shall create, as part of the office of fire marshal, a bureau of code enforcement consisting of a chief of the bureau and additional assistant fire marshals as the fire marshal determines necessary for the efficient administration of the bureau. The chief shall be qualified, by education or experience, in fire inspection, fire code development, fire code enforcement, or any other similar field determined by the fire marshal, and in administration, including the supervision of subordinates. The chief is responsible, under the direction of the fire marshal, for fire inspection, fire code development, fire code enforcement, and any other duties delegated to the chief by the fire marshal.

(2) The fire marshal, the chief deputy fire marshal, the chief of the bureau of code enforcement, or any assistant fire marshal under the direction of the fire marshal, the chief deputy fire marshal, or the chief of the bureau of code enforcement may cause to be conducted the inspection of all buildings, structures, and other places, the condition of which may be dangerous from a fire safety standpoint to life or property, or to property adjacent to the buildings, structures, or other places.

Mapping B: Department of Commerce; State Fire Marshal; Code Enforcement Bureau

Bureau-level: 1. Administering and enforcing the licensure and fire safety provisions of R.C. Chapter 3731 (Hotels), including R.C. §§ 3731.02 to 3731.21 and 3731.99.

2. Administering and enforcing the licensure and fire safety provisions of Chapter 3737, including R.C. §§ 3737.14, 3737.22(A)(1)(2) and (3),(D),(F) and (G), 3737.41, 3737.42, 3737.43, 3737.44, 3737.45, 3737.46, 3737.51, 3737.61, 3737.65, 3737.72 , 3737.73 and 3737.99 (B), (C), (E) and (F) and other selected R.C. provisions, including R.C. §§ 3701.82, 3721.02, 3721.03.2, 3721.07, 3722.02, 3722.04 and 3741.14.

3. Administering, developing and enforcing the state fire code promulgated under R.C §§ 3737.22(A)(1), 3737.82, 3737.83, 3737.84, 3737.85 and 3737.86 or other rules promulgated by the SFM pursuant to R.C. Chapters 3731, 3737 (except Bureau of Underground Storage Tank [BUSTR] matters described in R.C. §3737.81-98), 3741 or 3743.

4. Per R.C. § 3781.03(A), enforcing rules related to fire prevention promulgated pursuant to R.C. Chapters 3781 or 3791.

5. Per R.C. § 3737.22(A)(14), administering and enforcing R.C. Chapter 3743 (Fireworks) in accordance with applicable laws and SFM guidelines and procedures, including R.C. §§ 3743.02 to 3743.08, 3743.15 to 3743.25, 3743.40, 3743.44, 3743.45, 3743.50 to 3743.56, 3743.58, 3743.59, 3743.60 to 3743.68 (for licensing/Ohio Fire Code violations only), 3743.70, 3743.75, 3743.80 and 3743.99 (as it relates to licensing/Ohio Fire Code violations only). This enforcement authority does not include any grant of authority to any person in the Code Enforcement Bureau to arrest persons for violations of R.C. Chapter 3743 as described in R.C. §3743.68.

Potential policy statement: Only those employees assigned to the Bureau of Code Enforcement and engaged in processes, activities, and work duties associated with the bureau may access CPI of the bureau. All other access related to CPI within the agency or division shall be denied. Investigations in support of FIEB are exempt from ORC Chapter 1347 per ORC 1347.04.

Mapping C: Department of Commerce; State Fire Marshal; Fire, Explosives & Investigations Bureau

| |
|---|
| <p>Agency-level: ORC 121.02; 121.03; 121.04; 121.07; and 121.08; which establishes the Ohio Department of Commerce, its various divisions and their missions. ORC 1347.15 which defines how agencies must handle CPI and ORC 149.43 which defines how agencies must maintain public records.</p> |
| <p>Division-level: Pursuant to ORC 121 and 3737.22 (A)(4) Conduct investigations into the cause, origin, and circumstances of fires and explosions, and assist in the prosecution of persons believed to be guilty of arson or a similar crime; [...] The chief, among other duties delegated to the chief by the fire marshal, shall be responsible, under the direction of the fire marshal, for the investigation of the cause, origin, and circumstances of fires and explosions in the state, and for assistance in the prosecution of persons believed to be guilty of arson or a similar crime.</p> |
| <p>Bureau-level: Investigation of the cause, origin and circumstances of fires in Ohio and the arrest of and assistance in the prosecution of persons believed to be guilty of arson or a similar crime in accordance with R.C. §§ 2901.01(A)(11)(b), 3737.16, 3737.22(A)(4), (A)(13) and (C), 3737.22.1, 3737.24, 3737.25, 3737.26 (such as investigation of violations of R.C. §§2909.02, 2909.03, 2923.17 and associated statutes), 3737.27, 3737.28, 3737.29, 3737.31, 3737.32, 3737.33.1, 3737.62, 3737.63 and 3737.99 (A), (D) and (E). Pursuant to R.C. §3743.68(A) and (B), the investigation and arrest of a person for violations of R.C. §§ 3743.54.1, 3743.60, 3743.61, 3743.62, 3743.63, 3743.64, 3743.65 and 3743.66, seizures of contraband fireworks associated with such violations and 3743.99.</p> <p>Acts as Peace Officers in accordance with R.C. §§109.71(A)(23), 2935.01(B), 2935.03(A)(2) and applicable Department of Commerce and/or Division of State Fire Marshal policies.</p> |
| <p><i>Potential policy statement:</i> Employees serving as Peace Officers and their investigations are exempt from ORC. Chapter 1347 per ORC 1347.04.</p> |

Mapping D: Administrative access

| |
|--|
| <p>Agency-level: ORC 121.02; 121.03; 121.04; 121.07; and 121.08; which establishes the Ohio Department of Commerce, its various divisions and their missions. ORC 1347.15 which defines how agencies must handle CPI and ORC 149.43 which defines how agencies must maintain public records.</p> |
| <p>Division-level: Administrative staff may help support any program area as assigned and approved by the State Fire Marshal.</p> |
| <p>Bureau-level: <i>Example A:</i> A Data Administration Manager accesses CPI in the process of troubleshooting an eLicensing reporting problem.</p> <p><i>Example B:</i> A records manager accesses CPI while providing licensee information in support of one of the Board's program areas.</p> |

Mapping D: Administrative access

Potential policy statements: IT staff may require access to CPI while performing maintenance on agency information systems. Such access shall be limited to ensuring that the information systems are operating efficiently and effectively.

Records management staff may require access to CPI to support other program areas of the Division. This access shall be limited to ensuring that the Division's bureaus can efficiently and effectively access information in support of legitimate goals.

Mapping E: Non-routine inquiries

Agency-level: ORC 121.02; 121.03; 121.04; 121.07; and 121.08; which establishes the Ohio Department of Commerce, its various divisions and their missions. ORC 1347.15 which defines how agencies must handle CPI and ORC 149.43 which defines how agencies must maintain public records.

Division-level: Program area, *Executive staff*. answers non-routine inquiries.

Bureau-level: Director or his or her designee answers non-routine inquiry regarding a particular licensee, inspection, case, or record.

Potential policy statement: The Director of the Board or his or her designee may access CPI in the course of answering a non-routine inquiry. The reasons for: a) authorizing an employee to access this specific CPI and b) how such reasons directly relate to the state agency's exercise of its powers or duties must be documented.

Development of CPI access policies: Drafting

As each organizational component is mapped, the potential policy statements are collected and placed into a policy framework or standard policy template. Each of the tiered policy documents should have the numbered paragraphs for each of the following: 1) Purpose; 2) Scope; 3) Background; 4) References; 5) Policy (the statements themselves); 6) Procedure; 7) Revision History; 8) Definitions; 9) Related Resources; 10) Inquiries; and 11) Attachments.

Using Commerce at the agency level and the State Fire Marshal examples above at the lower levels, the following attachments are the draft policies that resulted from the process described above [attachments will be included in the final version of this document]:

Attachment 1: Ohio Department of Commerce Policy regarding CPI (overall agency-level draft).

Attachment 2: State Fire Marshal Policy regarding CPI (division-level draft).

Attachment 3: Bureau of Underground Storage Tank Regulation (bureau-level draft)

Attachment 4: Bureau of Code Enforcement (bureau-level draft)

Attachment 5: Fire, Explosives, and Investigations Bureau

Note that, while all three of the bureaus selected for this case study are under the Department of Commerce and the State Fire Marshal, each requires a separate policy. One bureau is mostly exempt from 1347.15 by the nature of its criminal investigations activity; another is not. The third, depending upon the activity, is occasionally exempt.

Technical Implementation of the Policy

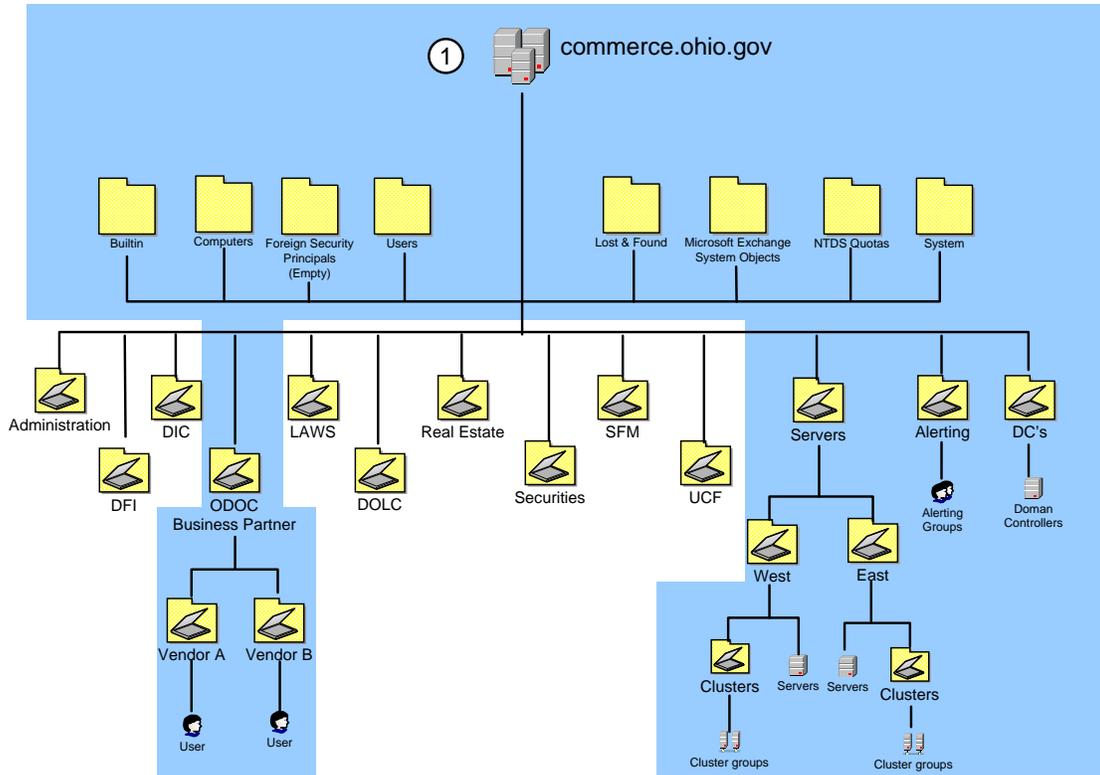
Policy implementation often requires activity in several areas. Direct dissemination of policies to employees requires communication and training efforts. And with policies that affect systems and software, certain activities require action by IT personnel. Access policies will almost certainly require IT personnel to use various security toolsets upon implementation, particularly in association with a Lightweight Directory Access Protocol (LDAP)-based network control method. Microsoft's Active Directory (AD) is a common example of such a directory and, like most, it can be structured to follow the organizational hierarchy that an agency has in place. As a result, IT personnel can easily translate access policies that have been crafted using the "top down" model into the proper access rights and group policies in Active Directory.

In addition, many security-layer software suites (Symantec, RSA, etc.) integrate with Active Directory to provide access control, authentication, and auditing capabilities to the systems they are deployed upon. Implementation of these systems will require a thought-out LDAP/AD deployment.

The following diagrams (made generic for this case study) were created by Commerce's network administrators while documenting the deployment of Active Directory. The areas highlighted under blue (Number 1, Attachment 1) can be covered by an agency-level access policy. Areas not highlighted must be covered by divisional- or bureau-level access policies. As a result, a complete correlation between the "top down model", the organizational structure, policy mappings, policy coverage, and the implementation of the LDAP/Active Directory implementation can be made.

Figure 7: Ohio Commerce Active Directory Structure

Active Directory Structure - Ohio Department of Commerce

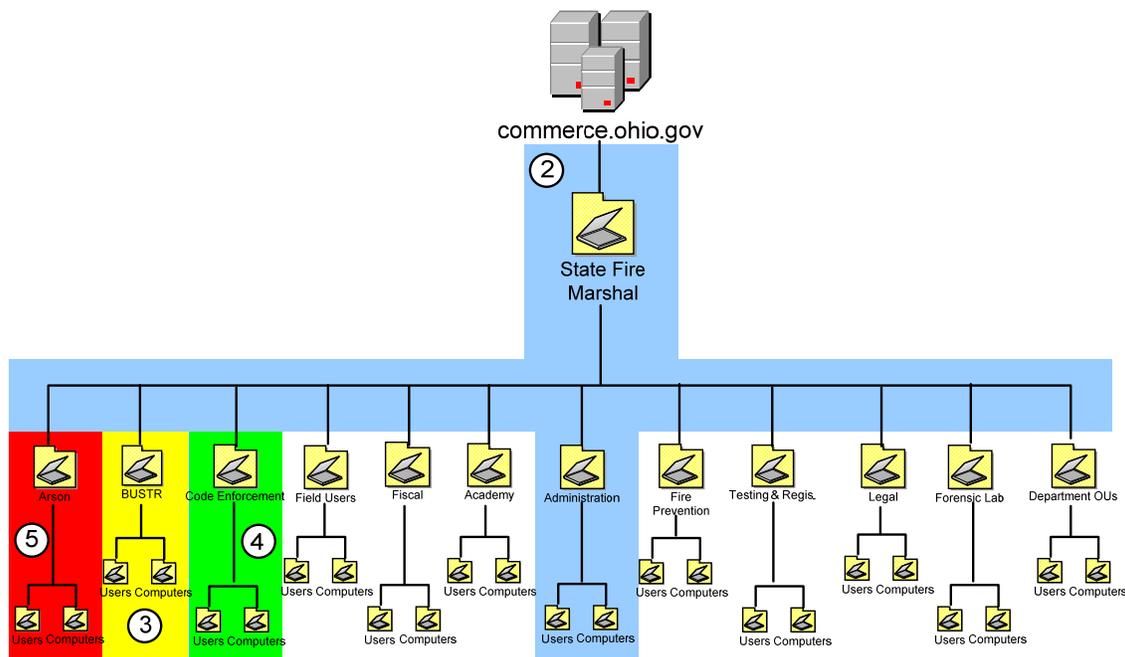


Each Division OU will Contain OUs for each of the Bureaus: Admins, Fiscal, Legal, Etc..
In the Bureaus there will be 3 or more additional OUs. Users, Computers, Field Staff (users & Comps)

Each division in the diagram shown above was further documented. In the example below, the State Fire Marshal is shown as the division with the mappings and draft policies in this case study. Per the mappings, areas highlighted in blue under Number 2 (Attachment 2) could be covered by a divisional access policy, whereas Arson (red, Number 5, Attachment 5) is governed by another policy - recall that the mapping for Arson / Fire, Explosives and Investigations Bureau concluded that this bureau was exempt from ORC 1347.15. The other bureau examples highlighted in yellow (Number 3, Attachment 3) and in green (Number 4, Attachment 4) would also have their own access policies per the mapping process.

Figure 8: State Fire Marshal Active Directory Structure

State Fire Marshal Active Directory Structure - Ohio Department of Commerce



Next Steps

Other, important “next steps” should be followed once the policies have been created and technical implementation has begun. These steps include: ITIL inclusion; infrastructure or continuous improvements; training; rule making process and regulatory reform efforts.

The Information Technology Infrastructure Library (ITIL) is a standards and documentation framework or method being adopted by many IT organizations and operations. Any access policies that are created should be referenced or included in the ITIL documentation.

Infrastructure changes or continuous improvements, especially those that result from efforts to properly handle CPI, should be planned and documented with reference to the policies. For example: a SAN expansion project implementing a logging capability necessary to support the issuance of access policies.

Training activities must be planned and implemented to ensure that the policies are communicated to employees and others in accordance with both ORC 1347 and the policies themselves.

The access policies will, once issued, form the basis for the creation of supporting rules and administrative code. The rule-making process is the primary next step to overall agency implementation of House Bill 648.

The current Administration has placed an emphasis on regulatory reform. A number of agencies have conducted rule and process reviews in regards to the Administration’s initiative and

process. Inclusion of access policy review in the regulatory reform process should be a next or reoccurring step. In fact, the regulatory reform process actually requires agencies to examine the need to collect any information in the process of being examined and to limit, where possible, the need to gather CPI.

Misuse of CPI

Misuse of CPI can trigger very serious consequences. Under ORC 1347.15 (G):

A person who is harmed by a violation of a rule of a state agency described in division (B) of this section may bring an action in the court of claims, as described in division (F) of section 2743.02 of the Revised Code, against any person who directly and proximately caused the harm.

In addition, ORC 1347.15 (H)(3) prevents state agencies from employing individuals who have been “convicted of or pleaded guilty to a violation of division (H)(1) or (2) of this section.”

What constitutes misuse of CPI? Some guidance on misuse of personal information is available under ORC 1347.10:

- Intentionally maintaining personal information that a person knows, or has reason to know, is inaccurate, irrelevant, no longer timely, or incomplete and may result in harm;
- Intentionally using or disclosing the personal information in a manner prohibited by law;
- Intentionally supplying personal information, using or disclosing for storage in, or using or disclosing personal information maintained in, a personal information system, that is false, or that the person has reason to know is false;
- Intentionally denying to an affected individual the right to inspect and dispute the personal information at a time when inspection or correction might have prevented harm.

Note that this guidance may not sufficiently describe all potential cases of misuse of CPI within your agency. Agencies should review the context in which employees access particular forms of CPI to determine if specific guidance needs to be developed and incorporated into security education and awareness programs.

