

State of Ohio

Role and Identity Management Resource Kit

Role and Identity Management Working Group

March 8, 2010

Preface

This document was created as a result of the research conducted by the Role and Identity Management Working Group under the Data Protection Subcommittee of the Multi-Agency CIO Advisory Council. Member agencies of the Working Group include:

Environmental Protection Agency	Job & Family Services	State Auditor
Health	Public Safety	Taxation
Insurance	Rehabilitation Services Commission	Transportation
		Workers' Compensation
		Youth Services

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 the Role and Identity Management Working Group is to address the requirements of Ohio Revised Code §1347.15 (B), that state agencies adopt as an administrative rule:

“Criteria for determining which employees of the state agency may access, and which supervisory employees of the state agency may authorize those employees to access, confidential personal information;”

Role and identity management provides a way to develop and maintain the criteria to access Confidential Personal Information (CPI). The authority for an agency to maintain and use CPI is typically defined in statute or other rules and regulations that govern the agency’s business processes. **Roles** provide a way to relate the functional tasks performed by state employees to these agency rules and regulations. **Identity** provides a means to accurately identify the individuals that access CPI, and to determine if this access is appropriate based on their role.

This resource kit, developed by the Role and Identity Management working group, is a compilation of documents that may assist agencies in developing a consistent approach to role and identity management. Specifically, the resource kit consists of the following:

- Two role process diagrams. These diagrams illustrate two potential ways to define and implement roles within an organization.
- A set of best practices related to role and identity management. These practices address the use of roles from a business perspective; the process for defining and documenting roles, or “role engineering”; and the ongoing maintenance of roles and identities. This section also includes a number of materials to support implementation of these practices:
 - A role handbook template that permits documentation of the relationship between roles and position descriptions, and to list the precise forms of CPI that each role may access.
 - An example of a role handbook that illustrates how the Ohio Administrative Knowledge System (OAKS) documents tasks associated with particular roles.
 - An example of a role matrix: a spreadsheet that complements the OAKS role handbook example above. Individual employees can be associated with corresponding roles using this spreadsheet.
 - A blank role matrix to be filled out by agencies.
 - A system administrator role matrix example: this matrix is used by an agency in conjunction with their data classification efforts. This document focuses on a) identifying sensitive table elements and b) the degree of access that system administrators have to these elements.

Table of Contents

The following is a list of all materials contained in this Resource Kit:

Preface.....	2
Overview.....	3
Table of Contents.....	4
Terms.....	4
Section A: Role Process Diagrams.....	6
Section B: Role and Identity Management: Best Practices.....	9
Role Handbook Template.....	9
OAKS Role Handbook Example.....	10
OAKS Role Matrix.....	12
Role Matrix Template.....	13
Role Matrix and Data Dictionary.....	14

Terms

The following terms are used throughout this document:

Confidential Personal Information (CPI) – As described in ORC 1347.15 (A)(1), CPI is 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 – Synonymous with **information stewards** for the purposes of this document. Persons from a business or program area who are responsible for classifying data and generating guidelines for its lifecycle management. 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.

¹All security- and privacy-related Ohio IT policies may be found at:
<http://www.privacy.ohio.gov/ohiopolicies/index.stm>.

Identity - The unique identifier for a user.

Identity management - Managing the creation, deletion or other limitations of identities for resources.

Identity verification - The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the Personal Identity Verification card or system and associated with the identity being claimed.

Information steward – See *data owner*.

Personal information – As defined in ORC 1347.01(E), “personal information” means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.

Role – A “role” is a collection of permissions. Users are granted membership into roles based on their competencies and responsibilities. Roles simplify the administration and management of privileges. Roles can be updated without having to customize the privileges of every user on an individual basis.

Role engineering - The process of defining roles.

Sensitive information – Refers to information that agencies have discretion to release and that could pose privacy or security risks. Certain agencies may use this term to refer to a category of non-public information larger than CPI.

System – As defined in ORC 1347.01, “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 – As defined in Ohio IT Policy ITP-B.1, “Information Security Framework,” users are defined as employees, contractors, temporary personnel and other agents of the state who administer or use privately-owned (if authorized) or state-owned computer and telecommunication systems on behalf of the state.

Section A: Role Process Diagrams

The diagrams in this section illustrate two potential workflows for developing and implementing roles within an organization. These workflows are a subset of an overall ORC 1347.15 implementation effort:

- Once an agency has identified **where** CPI is maintained through a data discovery and classification effort, and
- **why** access to this CPI is permitted through the development of access policies, then
- determine **who** can access CPI and **who can authorize** this access through role and identity management.

The documents and methods shown in the diagrams are discussed in greater detail throughout this resource kit. Use the workflows to provide context to an overall role and identity management effort.

Figure 1: Define and Document System Roles depicts business process stakeholders using two complementary approaches to identify and document roles: *top-down*, where agencies identify the roles necessary to support the organization’s processes, or *bottom-up*, where business processes are examined and roles are identified to support such processes. Roles serve as the criteria to determine which employees of the state agency may access CPI. A “role handbook” is used to document these roles and to identify relationships between roles and position descriptions.

Figure 1: Define and Document System Roles

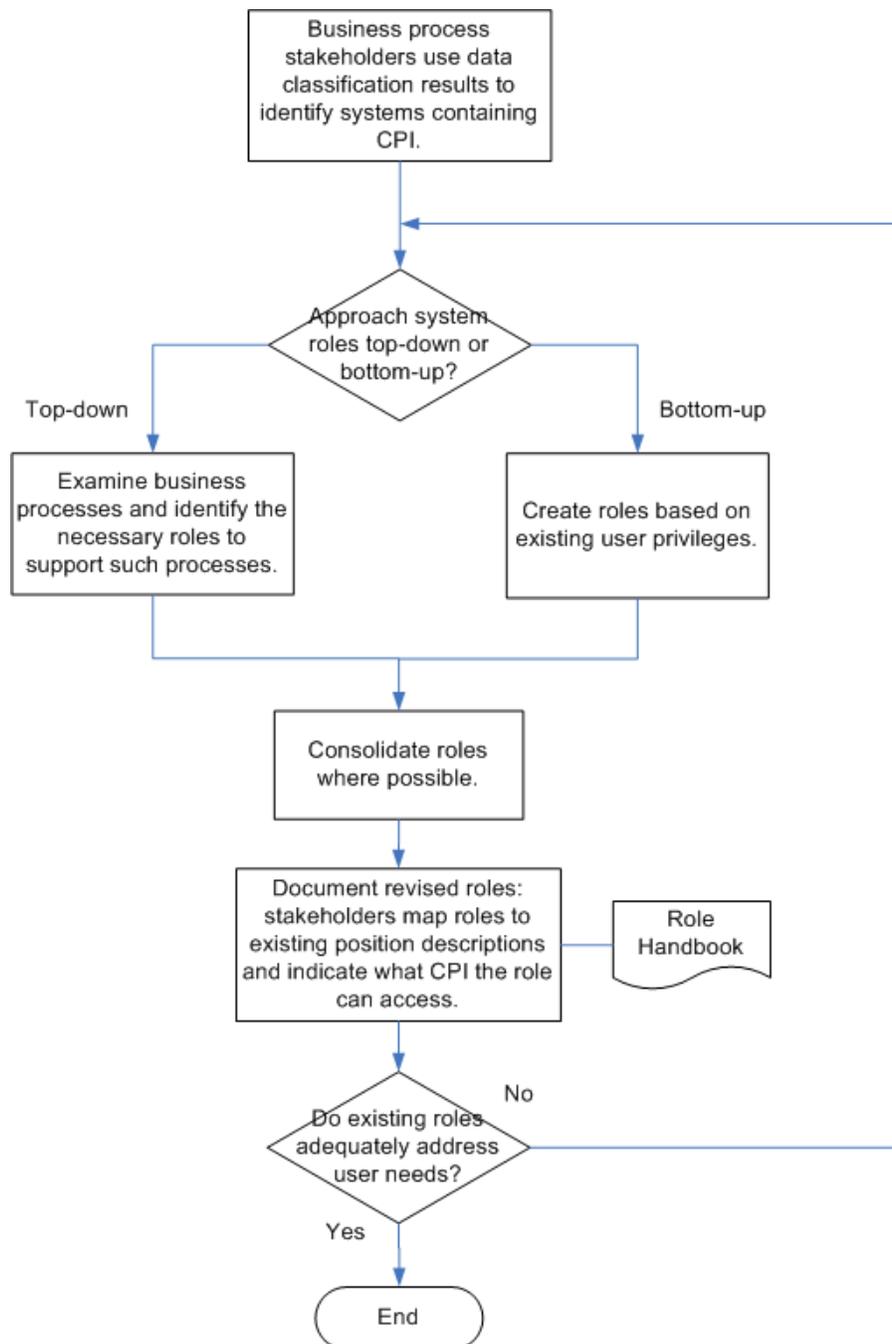
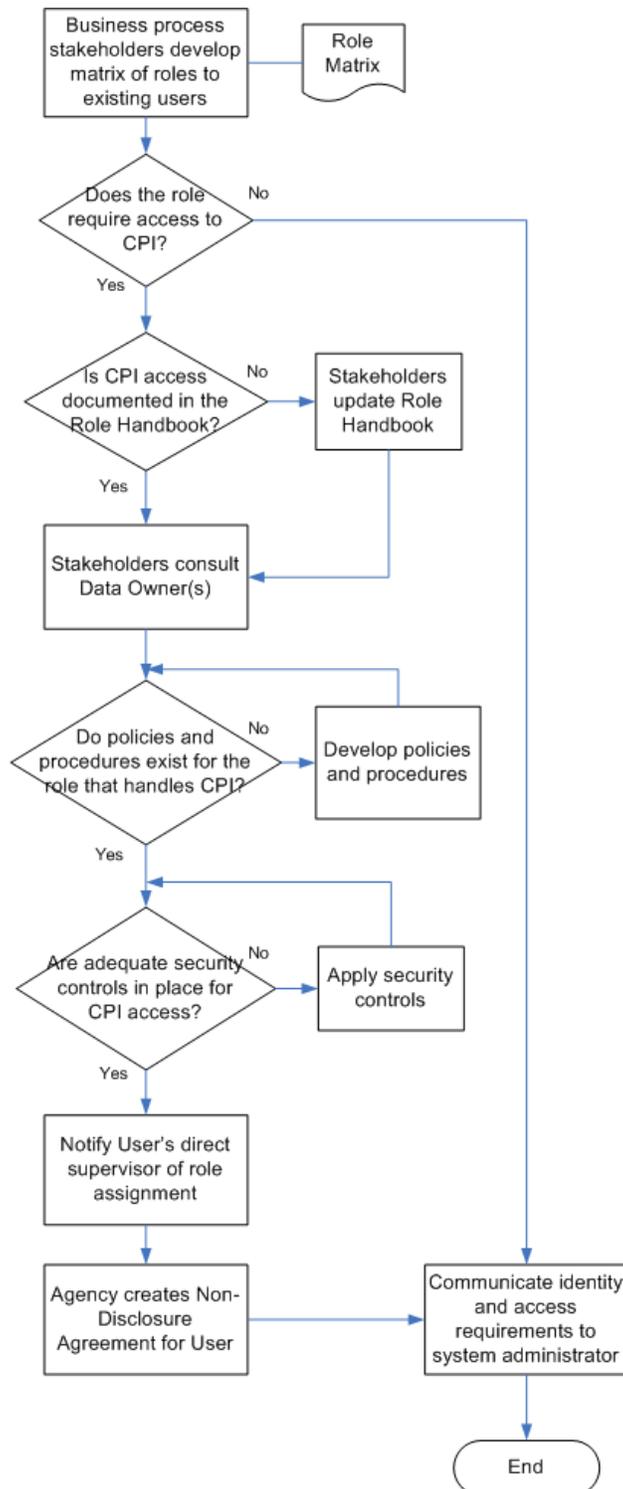


Figure 2: Implementation of Roles shows business process stakeholders using a role matrix to authorize access for specific users to systems containing CPI. Examples of both role handbooks and role matrices may be found in subsequent sections of this document.

Figure 2: Implementation of Roles



Section B: Role and Identity Management: Best Practices

Roles and Agency Business - Best Practices

- Prior to implementing roles, agencies should assemble a team of individuals from the legal, business and IT sections of the organization to guide the effort. An example team might include representatives from Human Resources, a business process stakeholder, legal counsel, and a system administrator who controls access to information systems. Create awareness that the IT department is not the sole “owner” of CPI or the roles that can access CPI.
- Even if information systems are not able to support role-based access, roles can still be defined for use in agency business processes. Create an agency role handbook that documents the tasks each agency role is to perform. See the following template and handbook excerpt for examples of such role documentation:

Role Handbook Template

This role handbook template provides an alternate way of documenting roles within a state agency. Human Resources managers or other appropriate agency personnel may use this form to document the relationship between roles and position descriptions, and to list the precise forms of CPI that the role may access. Suggested entries within the handbook would contain the following elements:

Role Name – Name of the agency role.

Description – A description of the business responsibilities associated with the role.

Map to Existing Position Description – The Human Resources position descriptions that may potentially fulfill this role.

Skills and Training – A description of the skills required for an individual to successfully perform the role, as well as the training necessary to handle particular functions, such as the proper handling of Confidential Personal Information.

Confidential Personal Information Access – List the electronic or paper forms of Confidential Personal Information that the role is permitted to access.

OAKS Role Handbook Example

This example is an excerpt of the OAKS Role Handbook and includes roles from one particular system module: *Asset Management*. Each role consists of a set of tasks that an individual may perform as a member of that role. Roles are not intended to reflect State of Ohio job titles. These roles were configured through a functional analysis of the agency's business processes. Each agency may opt to develop its own Role Handbook format so long as it accurately documents the user roles within the agency.

This handbook will be updated in the future as roles are added/deleted or modified.

AM – Asset Management Module

Agency AM Role – Asset Viewer

Tasks

- Reviewing asset information – including asset basic information, acquisition details, cost/book information, depreciation information, and accounting entries
- Reviewing capital lease asset information
- Reviewing parent/child relationships
- Searching for an asset
- Printing an asset

Agency AM Role – Asset Adjustment/Transfer Processor

Tasks

- Adjusting an asset's cost information
- Performing a cost addition
- Updating an asset's chartfield values
- Performing an InterUnit transfer
- Performing a re-categorization
- Reviewing an asset's cost/book information

Agency AM Role – Asset Retirement Processor

Tasks

- Retiring an asset
- Processing a disposal worksheet
- Reinstating an asset
- Reviewing an asset's cost/book information

Agency AM Role – Asset Maintenance Processor

Tasks

- Entering a maintenance event
- Entering a maintenance contract
- Reviewing maintenance history
- Entering a warranty
- Entering an insurance policy

Roles and Agency Business - Best Practices - continued

- Establish data owners for each information system and ensure that they are aware of the roles that can access that system's CPI.
- Create an exception process for when a user needs access to either CPI or a system containing CPI that is outside of their ordinary assigned role. Ensure that CPI access outside of the organization's routine activities is vetted through a formal process with the agency's data privacy point of contact and relevant information security officials.
- Encourage employees to understand their responsibilities in maintaining and accessing CPI.
- Establish a formal process for identifying the agency personnel authorized to access CPI. See **Figure 1: Define and Document System Roles** for an example of this process.
- Access to CPI maintained by an external state agency will at a minimum require: a) approval from the external agency data owner and b) approval from the employee's direct supervisor.
- Always record the approval of access to CPI. This approval may consist of either a signed agreement or an electronic record. See the following excerpt and templates for examples of such role documentation:

OAKS Role Matrix

This spreadsheet is used by OAKS in conjunction with the **OAKS Role Handbook Example** shown earlier to document the relation between individual employees and their corresponding roles. A full copy of this document may be found at: http://oakspmo.ohio.gov/extranet/Documents/Tasks/TEC/Task521_Attachment_B.xls. Each agency may develop its own Role Matrix document(s) so long as the document(s) accurately reflects the relation between individual employees and their corresponding roles.

CFO or Designee Name _____

(*) denotes required fields

								Asset Management (AM)				
* Last Name	* First Name	* Middle Initial	* OAKS EmplID	* Email Address	*Current OAKS FIN User (Y/N)	Default Business Unit (BU)	Additional Business Units (BUs) User Will Access	Agency Asset Viewer	Agency Asset Processor	Agency Asset Adjustment/Transfer Processor	Agency Asset Retirement Processor	Agency Asset Maintenance Processor
Doe	John	S	12345678	John.Doe@oaks.state.oh.us								

Role Matrix and Data Dictionary

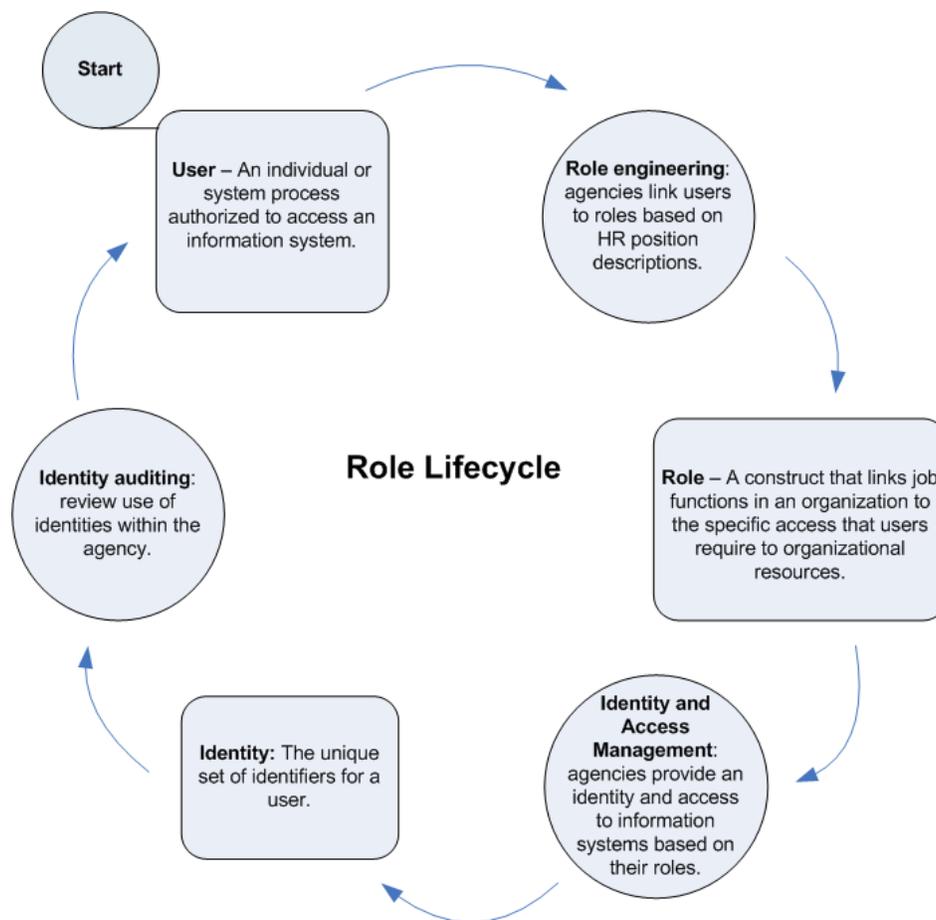
The matrix below is used by an Ohio agency to a) document the sensitivity of database information and b) identify the appropriate levels of access for system administrators or other “super users.” The matrix is often utilized whenever the agency undertakes a data classification effort. Individual data elements are identified as sensitive, and the level of access appropriate for each type of administrator is set to: Create, Read, Update or Delete. Each agency may develop its own Role Matrix and Data Dictionary document(s) so long as the document(s) accurately reflects the sensitivity of database information and identifies the appropriate levels of access for system administrators or other super users.

TABLE_NAME	COLUMN_NAME	DATA_TYPE	COLUMN_DESC	CPI (Y/N)	RETENTION SCHEDULE	Business Role(s)	Security Role(s)	Create	Read	Update	Delete
ADDRESS	ACTIVE_IND	NUMBER		N							
						Administrator	System_Administrator				
						Manager	System_Manager				
						Investigator	System_Investigator				
						Executive Reviewer	System_ExecutiveReviewer				
						System Admin	System_SysAdmin				
ADDRESS	ADDRESS_ADDTNL_INFO	VARCHAR2		N							
						Administrator	System_Administrator				
						Manager	System_Manager				
						Investigator	System_Investigator				
						Executive Reviewer	System_ExecutiveReviewer				
						System Admin	System_SysAdmin				

Role Engineering - Best Practices

- Review user categories and job functions to discover the roles that require access to CPI. Role engineering should ultimately connect users to roles, and help connect roles to identities based on agency access policies. The following diagram illustrates these terms and the business processes that tie them together:

Figure 3: Role Lifecycle



- Consider a “bottom up” or “top down” approach to the creation of roles. A bottom up approach involves deriving roles from existing groups or access control lists; a top down approach starts with an analysis of agency business processes and the creation of roles necessary to support these processes. Typically, a “top down” approach is more time-consuming, although a hybrid approach may sometimes be warranted to fully capture the different roles. See **Figure 1: Define and Document System Roles** for an example of this process.
- If available, use the agency’s CPI access policies to help identify roles within the agency. Such policies will likely speak to categories of agency workers who access CPI in a consistent manner. These categories may translate easily into roles.

- Role engineering produces optimal results where there is a large amount of roles with little complexity. These positions are typically found at the lower end of the organizational pyramid. The higher you proceed up the pyramid, the more complex roles become and the more difficult time you will have with role engineering.
- Operational functions are an excellent starting point for role engineering. More complicated functions may resist easy role categorization.
- Role engineering can be taken to an extreme. Having more roles than users is a strong indication that the organization has “over-engineered” roles. Over-engineering may lead to roles that are unnecessary to the organization, or may cause needless reassignment of users to roles.
- In creating roles, consider not only what CPI a user should access, but also how they access it. This may help identify changes necessary to the agency’s security architecture. For example, consistent need to transfer CPI by e-mail for a commonly used role may indicate a corresponding need for e-mail encryption.

Role Maintenance - Best Practices

- Identity verification, e.g., a periodic review of access control lists, is necessary to ensure that roles are still valid. Quarterly review of access is recommended as a best practice; annual review is necessary at a minimum. Role engineering is an ongoing process that involves continual fine-tuning of roles (see **Figure 3: Role Lifecycle**).
- Review roles for accuracy whenever:
 - New or modified job descriptions are created within the HR organization.
 - New people are hired or transferred within the organization.
 - Jobs of a temporary nature like projects or task forces emerge.
 - A business reorganizes, or forms strategic alliances or partnerships.
 - Unused roles are detected.
 - Changes to the IT environment occur, such as new hardware or a new information system.
- Do not automatically delete user IDs when provisioning users. Some applications require unused or outdated IDs for certain transactions. Also, do not reuse unique user IDs (i.e., globally unique identifiers) as this may prevent accurate logging of CPI access.

