COLORADO
Department of Health Care Policy & Financing

1570 Grant Street
Denver, CO 80203

# FY 2019-20 Cybersecurity Incentive Frequently Asked Questions

*February 2020* *FY 2019-20 Cybersecurity Incentive*

## Table of Contents



## General Background

As part of the FY 2019-20 County Incentives Program, the Cybersecurity Incentive asks county departments of human/social services to determine current compliance with five of the Colorado Information Security Policies.

The Department of Health Care Policy and Financing (HCPF), Colorado Department of Human Services (CDHS), and the Governor's Office of Information Technology (OIT) collaborated to create a deliverable template for counties to submit to HCPFCountyRelations@state.co.us by July 5, 2020.

**Definitions:**

- Option 2: Counties whose IT services are provided by OIT's contractor, Istonish
- Option 3: Counties who maintain their own IT services
- WMS: Workflow Management System (e.g. HS Connect, Boulder Connect, RMM-I, etc.)

*What are the Colorado Information Security Policies?*

The Colorado Information Security Policies are a set of cyber security policies developed by OIT based on federal requirements for public agencies.

*Why do counties need to comply with the Colorado Information Security Policies?*

The Department is working with counties to become compliant with the CISPs to ensure the protection of data that is stored, processed, and transmitted by counties as agents of the state. State agencies and state information systems must also be compliant with the CISPs.

*Which CISPs are included in the FY 2019-20 Cybersecurity Incentive?*

The deliverable for the FY 2019-20 Cybersecurity Incentive only focuses on five CISPs.

- **CISP-001:** Access Control
- **CISP-004:** Security Assessment and Authorization
- **CISP-005:** Configuration Management
- **CISP-006:** Contingency Planning
- **CISP-013:** Risk Assessment

It was determined that a narrower focus was needed for the first year of the Cybersecurity Incentive to make measuring compliance feasible. More CISPs may be included in future years.

*Which Option County is my county?*

An Option 2 county has physical devices like computers, servers, and routers provided by OIT through OIT's contract with Istonish.

Option 3 counties have their own IT support and provide their own devices.

If you are unsure what option county your county is, please reach out to HCPFCountyRelations@state.co.us.

*I am an Option 2 county. How will I know what questions are answered by Istonish?*

The state has identified questions that would be covered by Istonish. Those questions have been removed from Option 2 counties' deliverable, as long as they do not have other information systems that use data from state information systems.

If your county has another system that uses data from state information systems, such as a workflow management system, the Risk Assessment and Remediation Plan deliverable must take that system into account. Please see below for more detail.

*Our county uses a workflow management system. How does that change how we fill out the deliverable?*

If your county has created and owns a workflow management system or other system that connects to and downloads data from state information systems, the Risk Assessment and Remediation Plan deliverable must take that workflow management system into account, along with your local information system and business practices when connecting to state systems.

If your county uses a workflow management system created by another entity that is NOT a county, the Risk Assessment and Remediation Plan deliverable must take that workflow management system into account, along with your regular business practices when connecting to state systems.

If your county uses a workflow management system created by another county or state-provided EDMS, then you do not have to account for that workflow management system in your answers.

*Do I need to read and understand the five CISPs in order to fill out the Risk Assessment and Remediation Plan Deliverable?*

It is recommended that counties read and understand the policies, as provided in the "Requirements" column of the deliverable.

The "Business Translation" column can be used for further understanding.

## Risk Assessment and Remediation Plan Deliverable

*What is a Risk Assessment and Remediation Plan?*

A risk assessment is "a process of identifying risks to organizational operations (including mission, functions, image reputation), organizational assets, individuals, other organizations, and the state, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis."

A remediation plan, also called a plan of action and milestones, is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

The purpose of these documents is to identify areas for improvement and to determine how and when compliance can be reached.

*How do I complete the Risk Assessment and Remediation Plan deliverable?*

The Risk Assessment and Remediation Plan deliverable is a questionnaire to which counties should respond "yes" or "no" to each question.

If the county answers "no," the county must include that field in the remediation plan for the CISP.

Detailed directions can be found in the Operational Memo.
The completed deliverable must be turned in to HCPFCountyRelations@state.co.us by July 5, 2020.

*Who should be involved in filling out the answers to the Risk Assessment & Remediation Plan?*

The county department of human/social services is responsible for returning a completed deliverable to the Department. The county can consult anyone in their county to help with answers. For example, county security administrators, any contractor that provides IT services to your county, individuals who manage written policy and process, etc.

## CISP-001 Access Control

*What is Access Control?*

Access control is defined in this CISP as "typically logical controls designed into the hardware and software of a computing system."

Counties can think of access control in terms of policy and programming that allows county users access to their own systems, their workflow management systems, and protected information found in state systems like CBMS, CHATs, ACSES, Trails, etc.

A list of terms important for Access Control can be found in the Definitions section of this CISP. OIT also provides a full glossary of important CISP terms.

## CISP-004 Security Assessment & Authorization

*What is a Security Assessment?*

A Security Assessment is the process for testing or evaluating security measures to determine if they are adequate to protect data.

*Why do counties need Security Assessment and Authorization?*

Simply implementing security policies and procedures is not enough to make sure that data is protected. Organizations should also evaluate and test their policies and procedures to find out if there any policies/procedures that are missing, as well as whether their existing policies/procedures are sufficient to provide adequate data security.

## CISP-005 Configuration Management

*What is Configuration Management?*

Configuration Management is establishing and maintaining the integrity of IT products (like laptops, servers, or apps) and information systems through control of processes for creating, changing, and monitoring the set-up of those products and systems.

## CISP-006 Contingency Planning

*What is Contingency Planning?*

Contingency Planning concerns evaluating the risks to an organization's ability to continue routine operations, identifying which systems/processes are critical to routine operations, determining the maximum amount of acceptable downtime for critical systems/operations, determining required recovery point, e.g., restoring to a point in time no later than a specified timeframe, and developing plans to restore such systems/processes to routine operations in the event of a disruption.

Contingency Planning should consider a myriad of potential disruptions such as natural disasters, pandemic illness or other occurrences that impact the ability of staff to report to work, significant power outages that disrupt operations, system malfunctions or incidents that disrupt processing, etc.

Contingency planning is similar to emergency planning that counties perform for their communities on a regular basis, with a focus on emergency events concerning systems and technology.

## CISP-013 Risk Assessment

*What is Risk Assessment?*

Risk Assessment is the process of identifying risks to business operations (including mission, functions, image, reputation), assets, individuals, and the state, resulting from the operation of an information system. Risk assessment analyzes threats and vulnerabilities and mitigation through security controls planned or in place.

*Why is this CISP not included on the Option 2 Risk Assessment and Remediation Plan?*

Currently, most CISP-013 components for Option 2 counties are covered by the state or by Istonish.

**Department Contact:**

HCPFCountyRelations@state.co.us
Colorado.gov/hcpf/county-admin