COLORADO
Department of Health Care Policy & Financing

OPERATIONAL MEMO

TITLE:	**IMPLEMENTATION OF THE FY 2021-22 CYBERSECURITY INCENTIVE**
SUPERSEDES NUMBER:	**HCPF OM 20-081**
EFFECTIVE DATE:	**JULY 1, 2021**
DIVISION AND OFFICE:	**COMMUNICATIONS AND GOVERNMENT RELATIONS, POLICY, COMMUNICATIONS AND OPERATIONS OFFICE**
PROGRAM AREA:	**COUNTY RELATIONS AND ADMINISTRATION**
KEY WORDS:	**INCENTIVES, CYBERSECURITY, DELIVERABLE, COUNTY ADMINISTRATION**
OPERATIONAL MEMO NUMBER: HCPF OM 21-077 **ISSUE DATE: NOVEMBER 22, 2021** **APPROVED BY: RACHEL REITER**	

HCPF Memo Series can be accessed online: https://www.colorado.gov/hcpf/memo-series

Purpose and Audience:

The purpose of this Operational Memo is to issue guidance to county departments of human/social services regarding the deliverable requirements to earn the fiscal year (FY) 2021-22 County Incentives Program Cybersecurity Incentive.

Information:

The Cybersecurity Incentive is weighted at 20 percent of total County Incentives funding. Whether Cybersecurity Incentive funding is earned will be determined by the completion and submission of the deliverables described below.

Background:

The Colorado Department of Health Care Policy & Financing (HCPF), in partnership with the Governor's Office of Information Technology (OIT) and the Colorado Department of Human Services (CDHS) are working toward the goal of standardizing cybersecurity measures for human services agencies across the State of Colorado.

To accomplish this goal, the Department continues to work with county partners, CDHS and OIT on adherence to data security and privacy best practices, the Federal Health and Human Services Security Risk Assessment, and compliance with the Colorado Information Security Policies (CISPs).

To move towards compliance with these policies, the Department collected a baseline deliverable from county departments in FY 2020-21. The Department's review of this deliverable has identified some areas of high need across Colorado's counties that can be addressed within one Fiscal Year.

Deliverable Submission

For Option 2 Counties, deliverables to be submitted for review and approval by the Department to earn Cybersecurity Incentive funds are:

- Contingency Plan
- Incident Response Plan

Both deliverables must be submitted and approved to earn the Cybersecurity Incentive.

For Option 3 counties, deliverables to be submitted for review and approval by the Department to earn Cybersecurity Incentives funds are:

- Contingency Plan
- Incident Response Plan
- System Security Plan

All three deliverables must be submitted and approved to earn the Cybersecurity Incentive.

Counties who responded **"yes"** that they *do have* one or more of these plans will be asked to submit them to the **Department by December 15, 2021** for review and approval by the Department. If the county who answered **"yes"** that they do have these plans, but cannot produce one or all of these documents, the county should inform the Department at hcpf_countyrelations@state.co.us.

If the county submits all of the plans by December 15, 2021 and all of the plans are approved, the county will have earned the Cybersecurity Incentive for FY 2021-22.

If one or more of the plans are **not** approved, the county will have until **June 15, 2022** to update and re-submit.

Counties who responded **"no"** that they *do not* have one or more of the above plans will have until **June 15, 2022** to create and submit the plans.

The Department will share the reviewed and approved county-submitted plans as examples for other counties to use as a basis for their own plan development.

Counties may not directly copy the approved plan from another county but should use the approved plans as a starting point to adapt to their own county.

Contingency Plan

A Contingency Plan will be reviewed to include at least the following criteria based on CISP-006:

- Identifies essential mission(s) and business functions and associated contingency requirements.
- Provides recovery objectives, restoration priorities and metrics.
- Addresses contingency roles, responsibilities, and individuals' contact information.
- Plans for the resumption of essential missions and business functions.
- Identifies critical technical and operational assets that support essential missions and functions.
- Addresses eventual, full Information System restoration without deterioration of the security safeguards originally planned and implemented.
- Ensures the plan is reviewed and approved by key business and Information System leaders or their designees.

All counties **not** listed below will have until **June 15, 2022** to develop a Contingency Plan.

If your county answered **"yes"** on the question 107 (CISP-006 9.1.1) of the FY 2020-21 deliverable, your county is listed below. Please turn in your Contingency Plan deliverable by **December 15, 2021**.

Adams	Denver	Grand
Arapahoe	Douglas	Gunnison
Broomfield	El Paso	Hinsdale
Clear Creek	Elbert	Jackson
Crowley	Fremont	Jefferson

Kiowa	Mineral	Rio Grande
Kit Carson	Montezuma	Routt
Lake	Otero	Summit
La Plata	Park	Teller
Las Animas	Pitkin	Weld
Logan	Prowers	
Mesa	Pueblo	

Incident Response Plan

An Incident Response Plan will be reviewed to include at least the following criteria based on CISP-008:

(a) Serves as a roadmap to handle information security incidents;
(b) Describes the structure of the incident response process;
(c) Documents the incident response team roles, resources, and responsibilities;
(d) Provides a high-level approach for how the incident response processes fit into the overall organization;
(e) Meets the unique requirements of the ITSP, which relate to mission, size, structure, and functions;
(f) Defines reportable incidents; and
(g) Provides metrics for measuring the incident response capability within the ITSP.

All counties **not** listed below will have until **June 15, 2022** to develop an Incident Response Plan.

If your county answered **"yes"** on question 166 (CISP-008 9.6.1) of the FY 2020-21 deliverable, your county is listed below. Please turn in your deliverable by **December 15, 2021**.

Adams	Denver	El Paso
Arapahoe	Douglas	Grand
Clear Creek	Eagle	Gunnison

Hinsdale	Mesa	Routt
Jackson	Mineral	Saguache
Jefferson	Montezuma	San Juan
Kiowa	Park	Summit
Kit Carson	Pitkin	Teller
La Plata	Prowers	Weld
Las Animas	Pueblo	

System Security Plan – OPTION 3 ONLY

A System Security Plan will be reviewed to include at least the following criteria based on CISP-017:

- Is consistent with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security categorization of the information system including supporting rationale;
- Describes the operational environment for the information system and relationships with, or connections to, other information systems;
- Provides an overview of the security requirements for the system;
- Identifies any relevant overlays, if applicable; and
- Describes the security controls in place or planned for meeting those requirements including a rationale for custom configuration decisions.

All counties **not** listed below will have until June 15, 2022 to develop a System Security Plan.

If your county answered **"yes"** on question 368 (CISP-017 9.5.1) of the FY 2020-21 deliverable, your county is listed below. Please turn in your deliverable by **December 15, 2021**.

Adams	Broomfield	El Paso
Arapahoe	Denver	Jefferson

La Plata	Montezuma	Routt
Mesa	Pitkin	Weld

Counties with HCPF Cybersecurity Grants

For counties who have cybersecurity grants provided by HCPF for FY 2021-22, the county cannot code efforts by the grantee or the contractor to create the policies listed within this memo to the CFMS code for the HCPF County Grant and thereby earn the Cybersecurity Incentive.

Attachment(s):

County Cybersecurity Webpage

Department Contact:

HCPF_CountyRelations@state.co.us