COLORADO
Department of Health Care
Policy & Financing

OPERATIONAL MEMO

TITLE:	**IMPLEMENTATION OF THE FY 2020-21 CYBER SECURITY INCENTIVE**
SUPERSEDES NUMBER:	**HCPF OM 19-036, HCPF OM 20-011**
EFFECTIVE DATE:	**JULY 1, 2020**
DIVISION AND OFFICE:	**COMMUNICATIONS AND GOVERNMENT RELATIONS, POLICY, COMMUNICATIONS & ADMINISTRATION OFFICE**
PROGRAM AREA:	**COUNTY RELATIONS AND ADMINISTRATION**
KEY WORDS:	**INCENTIVES, CYBER SECURITY, 2020-21, COUNTY INCENTIVES PROGRAM**

OPERATIONAL MEMO NUMBER: HCPF OM 20-081
ISSUE DATE: AUGUST 6, 2020
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 memo is to clarify to county departments of human/social services the deliverable requirements and necessary information to earn the fiscal year (FY) 2020-21 County Incentives Program Cyber Security Incentive.

Background Information

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 cyber security 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 and compliance with the Colorado Information Security Policies (CISPs).

To move towards statewide compliance with the CISPs and data privacy, a baseline measurement of current cyber security and data privacy practices is needed. The measurement will be completed in increments through a Risk Assessment and

Remediation Plan deliverable. For the FY 2020-21 Cyber Security Incentive, this deliverable is due on July 5, 2021.

The Cyber Security Incentive is weighted at 30 percent of total County Incentives funding. Whether Cyber Security Incentive funding is earned will be determined by the completion and submission of the Risk Assessment and Remediation Plan deliverable.

The Risk Assessment and Remediation Plan deliverable is the only deliverable for the FY 2021-21 Cyber Security Incentive.

Risk Assessment and Remediation Plan Deliverable

The Risk Assessment & Remediation Plan is based upon the federal Health & Human Services Risk Assessment, the Colorado Information Security Policies, and the standard Remediation Plan used by OIT. Since it is imperative that the Department, CDHS and OIT have a thorough understanding of what CISP compliance would look like in each county to accurately measure compliance, a Security Practices Workgroup was created with HCPF, CDHS, and OIT representatives.

Last fiscal year, five of the 18 CISPs were assessed. For FY 2020-21, the remaining CISPs will be newly assessed.

- CISP-002: Security Awareness and Training
- CISP-003: Audit and Accountability
- CISP-007: Identification and Authentication
- CISP-008: Incident Response
- CISP-009: System Maintenance
- CISP-010: Media Protection
- CISP-011: Physical and Environmental Protection
- CISP-012: Personnel Security
- CISP-014: System and Services Acquisition
- CISP-015: System and Communications Protection
- CISP-016: System and Information Integrity
- CISP-017: Security Planning
- CISP-018: Acceptable Use Policy (AUP)

Additionally, 57 questions on data privacy have been added to the county risk assessment from the federal U.S. Department of Health and Human Services (HHS) Risk Assessment.

Each county's responses from the five CISPs assessed in fiscal year 2019-20 Risk Assessment and Remediation Plan will be included on this year's deliverable. If the county's responses have changed, the previous year's answers should be updated. The five CISPs from the previous year include:

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

If your county did not complete the Risk Assessment & Remediation Plan deliverable for FY 2019-20, the questions from that deliverable must be answered in the FY 2020-21 Risk Assessment and Remediation Plan in order to earn this year's incentive funding.

There is no template for this fiscal year's Risk Assessment and Remediation Plan deliverable. Each county will have their own deliverable with the responses from last fiscal year included. Each county will have this fiscal year's deliverable sent directly to their county human/social services director, secondary director, and any contacts as requested by county leadership.

The Risk Assessment and Remediation Plan questions should be answered regarding county's local information system, workflow management systems, if applicable, the county's written policies and practices, and the county's use of and access to all State Information Systems, including the Colorado Benefits Management System (CBMS), Child Care Automated Tracking System (CHATS), Automated Child Support Enforcement System (ACSES), Trails, etc.

This deliverable is due **July 5, 2021**.

Option 2 County Instructions

If your county's IT services are provided by Istonish, then the FY 2020-21 Option 2 Risk Assessment and Remediation Plan Deliverable will be sent to your county director, secondary director, and any additional contacts identified by county leadership. The deliverable has been edited to exclude questions that are solely answerable by OIT or Istonish, on behalf of option 2 counties.

The deliverable will include:

- New questions from 12 of the 17 Colorado Information Security Policies (CISPs)
- Data privacy questions from the federal Health and Human Services (HHS) Risk Assessment

- Your county's responses from the previous fiscal year's assessment of five of the 17 CISPs

If any of your county's responses to the questions answered in the previous fiscal year have changed, the responses should be updated.

If your county did not complete the Risk Assessment & Remediation Plan deliverable for FY 2019-20, the questions from that deliverable must be answered in the FY 2020-21 Risk Assessment and Remediation Plan.

To fill out the deliverable:

- Answer "Yes" or "No" to each question, or "N/A" **only** where the N/A option is offered as a response.
- Fill out the remediation plan in the county response section addressing any fields where the answer was "No."
- Provide any additional context in the comments section.

Answer the questions regarding your county's written policies and procedures, business processes and use of all state systems, including CBMS, CHATS, ACSES, Trails, etc.

Submit the completed deliverable by **July 5, 2021**.

Option 3 County Instructions

If your county provides its own IT services, then the FY 2020-21 Option 3 Risk Assessment and Remediation Plan Deliverable will be sent to your county director, secondary director, and any additional contacts identified by county leadership.

The deliverable will include:

- New questions from 12 of the 17 Colorado Information Security Policies (CISPs)
- Data privacy questions from the federal Health and Human Services (HHS) Risk Assessment
- Your county's responses from the previous fiscal year's assessment of five of the 17 CISPs

If any of your county's responses to the questions answered in the previous fiscal year have changed, the responses should be updated.

- Answer "Yes" or "No" to each question, or "N/A" **only** where the N/A option is offered as a response.

- Fill out the remediation plan in the county response section addressing any fields where the answer was "No."
- Provide any additional context in the comments section.

Answer the questions with regard to your county's local information system, Workflow Management System and your county's business processes and use of all state systems, including CBMS, CHATS, ASCES, Trails, etc.

Turn in the completed deliverable by **July 5, 2021**.

Resources

The Risk Assessment and Remediation Plan deliverable includes a document library and glossary to help answer questions about the documents.

Throughout the fiscal year, the Department will collect questions asked by county and IT partners regarding the Risk Assessment and Remediation Plan deliverable and will develop a fiscal year 2020-21 Cyber Security FAQ. Additionally, the Department will schedule support calls for Option 2 and Option 3 counties to review the deliverable and answer questions.

The times and dates of these support calls will be sent to county directors, county secondary directors, and any additional county contacts identified or sent to HCPF_CountyRelations@state.co.us.

Attachment(s):

None

Department Contact:

HCPF_CountyRelations@state.co.us