Schedule 13
Funding Request for the 2013-14 Budget Cycle

Department: Department of Public Safety
Request Title: HSEM, Critical Infrastructure and Continuity of Operations Request
Priority Number: R-2

Dept. Approval by: Teresa Y Anderle 10/25/12 Date

OSPB Approval by: 10/25/12 Date

- [x] Decision Item FY 2013-14
- [ ] Base Reduction Item FY 2013-14
- [ ] Supplemental FY 2012-13
- [ ] Budget Amendment FY 2013-14

Line Item Information	Fund	FY 2012-13 1 Appropriation FY 2012-13	FY 2012-13 2 Supplemental Request FY 2012-13	FY 2013-14 3 Base Request FY 2013-14	FY 2013-14 4 Funding Change Request FY 2013-14	FY 2014-15 6 Continuation Amount FY 2014-15
Total of All Line Items	**Total**	-	-	728,669	74,332	92,018
	FTE	-	-	8.0	0.8	1.0
	GF	-	-	128,669	74,332	92,018
	CF	-	-	-	-	-
	HUTF	-	-	-	-	-
	RF	-	-	-	-	-
	FF	-	-	600,000	-	-
(6) Division of Homeland Security and Emergency Management Office of Preparedness	**Total**	-	-	728,669	74,332	92,018
	FTE	-	-	8.0	0.8	1.0
	GF	-	-	128,669	74,332	92,018
	CF	-	-	-	-	-
	HUTF	-	-	-	-	-
	RF	-	-	-	-	-
	FF	-	-	600,000	-	-

Letternote Text Revision Required? Yes: ☐ No: ☑ **If yes, describe the Letternote Text Revision:**

Cash or Federal Fund Name and COFRS Fund Number:
Reappropriated Funds Source, by Department and Line Item Name: N/A
Approval by OIT? Yes: ☐ No: ☐ **Not Required:** ☑
Schedule 13s from Affected Departments: N/A
Other Information:

This page was intentionally left blank.

DEPARTMENT OF PUBLIC SAFETY

FY 2013-14Funding Request
November 1, 2012

John W. Hickenlooper
Governor

James H. Davis
Executive Director

Signature Date

Department Priority: R-2
Critical Infrastructure & Continuity of Operations Request

Summary of Incremental Funding Change for FY 2013-14	Total Funds	General Fund	FTE
Critical Infrastructure & Continuity of Operations	$74,332	$74,332	0.8

Request Summary:
The Department requests $74,332 General Fund in FY 2013-14 and $92,018 in FY 2014-15 and beyond to provide funding for 1.0 FTE in the Division of Homeland Security & Emergency Management (DHSEM) to coordinate and manage all critical infrastructure protection activities for State-owned facilities and other key resources, as well as update and administer the State's continuity of operations/continuity of government programs and processes. This proposal will lead to greater resiliency within State government by ensuring that it is able to function and deliver vital services following a disaster or other critical incident. It also ensures that these two core functions will receive continuous oversight and development given their importance to the State's security posture in Colorado.

Problem or Opportunity:
Critical infrastructure protection is vital to the safety and security of Coloradoans and the economy. Critical infrastructure has been defined by the U.S. Department of Homeland Security (DHS) as the "…assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof." Examples of critical infrastructure include dams, power plants, electrical grids, information systems, military defense facilities, water treatment facilities, and transportation hubs like Denver International Airport. Threats to critical infrastructure are ubiquitous, requiring the State to remain adaptive and proactive in protecting its human and capital assets. While most critical infrastructure is owned by the private sector, the State maintains an array of facilities, systems, human capital, and other key resources that if compromised would seriously disrupt or cripple government operations. DHSEM currently maintains an inventory of 43 critical infrastructure sites in Colorado that are considered vital to State and National Security interests. The identity and whereabouts of these sites remains classified. In addition, there are over 3,800 additional critical infrastructure sites in Colorado whose disruption could pose serious risks to local communities. Lastly, State statute specifies that DHSEM is responsible for coordinating all protection-related activities for critical infrastructure, but no FTE have been allocated to ensure development, coordination, and oversight of this vital program.

Likewise, the continuity of operations and continuity of government (COOP/COG) program for the State of Colorado is fragmented, inconsistent, and not centrally managed. This makes it difficult to know which State agencies have plans and which don't. It is also unclear whether state agencies are training and exercising those plans to ensure a higher margin of readiness. COOP/COG is considered a staple of good government and may be the deciding factor of whether or not the State can perform vital functions and continue to deliver essential services to local government and citizens following a disaster or other critical incident. Without the resources and expertise to centrally manage this program for the State, resiliency of State operations will be more a product of chance rather than thoughtful determination.

Brief Background:
Critical infrastructure protection (CIP), as it pertains to incoming threat reporting and information sharing, is currently administered by the Office of Prevention and Security (OPS) within the Division of Homeland Security & Emergency Management. However, the focus is principally on threats as opposed to helping owners and operators develop resilient systems. Engaging private industry in critical infrastructure/key resource protection is vital to the local economy, the safety and security of local citizens, and the continuity of core government functions and services.

DHS recognizes eighteen critical infrastructure sectors, including water, information technology, energy, and government facilities. When threats are identified, to the government facilities sector in particular, they may have an immediate and cascading impact on State's facilities, employees, and the services provided by those agencies. Government and private industry can ill afford to discount the importance of critical infrastructure protection—and the need to be prepared for myriad threats, especially threats related to cyber. Because there are no full-time resources yet devoted to CIP, the scope and reach of the program is severely limited, thereby increasing the State's risk. Critical infrastructure protection has been, and continues to be, a core responsibility of the Department, and as Colorado law makes clear, the Office of Preparedness (OP) is obligated to, "…coordinate protection activities among owners and operators of critical infrastructure and other tribal, state, local, regional, and federal agencies in order to help secure and protect critical infrastructure within the state" (Section 24-33.5-1604(5)(f),C.R.S.). The core elements of a sustainable and robust critical infrastructure protection program include:

- Partnerships and collaboration
- Assessing and reducing vulnerability
- Threat and hazard identification, prioritization and mitigation
- Education and awareness
- Efficient use of resources

These principles serve as the starting point for program development. Without adequate resources, the Office of Preparedness (OP) will be unable to build resiliency within and among both privately owned and State government agencies and facilities. Vulnerability assessments previously conducted by peace officers on the State Capitol, CBI Headquarters, and Department of Revenue facilities cannot be replicated in the future without resources necessary to prevent and protect against threats and hazards that threaten State government.

The recent High Park and Waldo Canyon fires highlighted not only the vulnerability of local citizens, but taxed the State's ability to respond and recover from simultaneous, large-scale incidents. While natural hazards such as wildfire are prevalent and reoccurring, technological and man-made disasters can be equally devastating. The threats and hazards faced by Colorado are constantly evolving. To be effective, OP must ensure that the COOP/COG plans and processes are well developed and executed across the entire spectrum of State government. Colorado statute stipulates that the Executive Director of the Department adopt rules and provide guidance to State departments and agencies on continuity of

operations (Section 24-33.5-1609, *C.R.S.*). These rules are then to be incorporated into the State Emergency Operations Plan.

The former Governor's Office of Homeland Security (GOHS) devoted one full-time, grant-funded position to administer the program, but the position was eliminated back in 2008, and the program has been dormant ever since vital institutional knowledge has been lost in the process. This is not to say that State agencies have no COOP/COG plans in place. Many in fact do. But, false starts have negatively impacted the State's COOP/COG program.

After the dissolution of GOHS pursuant to Executive Order 2011-030, and with the creation of the new Division of Homeland Security & Emergency Management pursuant to HB12-1283, the Department has taken a fresh look at the program and determined that major steps must to be taken to rejuvenate the program to ensure that it is properly administered and sustainable over the long-term. The depth and breadth of the COOP/COG program directly influences the resiliency of government institutions following a disaster. There also needs to be better coordination and consistency in how these plans are developed, trained and exercised.

Proposed Solution:
In order to institutionalize these programs, 1.0 FTE is needed to ensure resiliency of government institutions and the ability to function and deliver key services in times of need.

Alternatives:
Critical infrastructure protection (CIP), directed foremost toward lifeline infrastructure and State facilities, is a critical component of the State and National Homeland Security Strategy. CIP is a shared responsibility between the government and private industry across all 18 critical infrastructure/key resource sectors. When it comes to the Government Facilities sector, responsibility to prevent, protect, and mitigate against threats and hazards lies squarely with the State. Nevertheless, one alternative to funding this proposal is to discontinue the CIP program entirely, relying simply on information sharing and current threat reporting capabilities already performed by OPS as opposed to program development, hazard/risk mitigation, and use of assessment methodologies.

The State could rely upon direct Federal support of CIP activities. The U.S. Department of Homeland Security (DHS) has assigned a Protective Security Advisor (PSA) to the State of Colorado. The PSA has long been a vital partner, and their knowledge and expertise of CIP matters is unparalleled. But, the PSA is first and foremost a Federal employee. They operate with certain limitations and are responsible for meeting Federal performance objectives set by the Infrastructure Protection Directorate (IP) at DHS. While the PSA remains a vital partner to the State, they should not be counted on to establish and maintain a State CIP program, especially one directed first and foremost toward State facilities and other key State resources.

Homeland security grant funding is often considered a viable alternative to the use of General Fund, but concerns over sustaining come to the forefront anytime the discussion revolves around state-mandated activities, which should be supported by State Funds not Federal funds. Moreover, grant funds cannot be used to fund traditional response activities, such as when an incident occurs or a credible threat is received and the State CIP coordinator is required to interface and assist State agencies with rolling out protective measures. In short, restrictions on the use of Federal grant funds make this funding source impractical for sustaining traditional state activities such as COOP/COG and CIP.

For COOP/COG, the only alternative, outside of not fulfilling the Department's statutory mandate, would be to apply available grant funding. However, using grant monies for activities or functions that are required by state law is problematic.

Anticipated Outcomes:
If funded, the program will:

- Develop and sustain a State critical infrastructure protection program based upon risk.
- Establish a central point of accountability for the protection of State human and capital assets.
- Reduce the vulnerability of State facilities, systems and networks, employees, and other key State resources through identification of threats and hazards.
- Develop plans and procedures to prevent, protect, and mitigate against threats and hazards.
- Ensure that CIP becomes a central feature of the State Homeland Security Strategy.
- Improve outreach, information sharing, and develop partnerships within and between state agencies and private industry.
- Develop consistent and uniform COOP/COG plans and procedures for all State agencies, and ensure that maintenance, training, and exercise elements are built into the plans.
- Prioritize vulnerabilities identified through the COOP/COG planning process and develop corrective action plans to ensure continuity of key functions and services.
- Improve education and awareness of threats and hazards affecting the State.

Assumptions for Calculations:
The transfer or consolidation of existing FTE pursuant to HB-1283 into the new Division of Homeland Security and Emergency Management did not include the 1.0 FTE requested here to maintain both the State's critical infrastructure and COOP/COG programs. This request is in recognition of the fact that these programs require dedicated FTE and other funding sources do not provide the level of efficacy and sustainment needed over the long-term.

The 1.0 FTE requested represents the minimum number of staffing needed to develop and maintain the COOP/COG and critical infrastructure protection programs and fulfill the Department's statutory obligations. For detailed funding calculations, see Attachment A.

Consequences if not Funded:
Without dedicated FTE, both programs will remain dormant. Existing FTE within the division cannot assume the duties of CIP or COOP/COG program activities due to the rigorous training and experience required of the positions and the time investment needed to properly develop and sustain the programs over the long term.

Moreover, CIP and COOP/COG are the basic building blocks of any State homeland security program. Without these programs, the State risks exposure to threats and hazards that are entirely preventable provided prevention and protection measures have been instituted, which these programs aim to do on a statewide basis. Colorado has recently experienced several natural disasters, but technological and man-made hazards exist as well. Preparedness cannot wait until after a disaster occurs. By then it is too late. The State must be proactive and demonstrate its commitment to building resiliency in all levels of State government.

Impact to Other State Government Agency:
No financial impact on other agencies.

Relation to Performance Measures:
For the CIP program, this proposal would allow OP to work toward certain measures, namely increasing the number of critical infrastructure sites added to the Automated Critical Asset Management System (ACAMS), attend vital information-sharing meetings with key partners, and conduct outreach with the Protective Security Advisor from DHS.

Current Statutory Authority or Needed Statutory Change:

The statutory authority requiring the division to perform critical infrastructure protection activities can be found at 24-33.5-1604(5)(f) *C.R.S., The Division shall also: Coordinate protection activities among owners and operators of critical infrastructure and other tribal, state, local, regional, and federal agencies in order to help secure and protect critical infrastructure within the state.*

The statutory authority requiring the Executive Director of CDPS to administer and coordinate COOP/COG activities can be found at 24-33.5-1609, *C.R.S.* in part, *(1)The director shall adopt rules concerning the continuity of state government operations to provide guidance to state departments and agencies in developing viable and executable contingency plans for continuity of operations.*

Calculation Assumptions:

Personal Services -- Based on the Department of Personnel and Administration's July 2012 Annual Compensation Survey Report, a GPVI at the BOTTOM of the pay range will require a monthly salary of $6,041.

Operating Expenses -- Base operating expenses are included per FTE for $500 per year. In addition, for regular FTE, annual telephone costs assume base charges of $450 per year.

Standard Capital Purchases -- Each additional employee necessitates the purchase of a Personal Computer ($900), Office Suite Software ($330), and office furniture ($3,473).

General Fund FTE -- New full-time General Fund positions are reflected in FY 2012-13 as 0.75 FTE to account for the pay-date shift and later date of hire.

Expenditure Detail		FY 2013-14		FY 2014-15	
Personal Services:		FTE	$	FTE	
	Monthly Salary				
General Professional VI	$ 6,041	0.75	54,369	1.0	72,492
PERA			5,518		7,358
AED			1,957		2,900
SAED			1,767		2,718
Medicare			788		1,051
STD			96		128
Health-Life-Dental			4,421		4,421
Subtotal Position 1, #.# FTE		0.75	**$ 68,916**	1.0	**$ 91,068**
Subtotal Personal Services		0.8	**$ 68,916**	1.0	**$ 91,068**
Operating Expenses					
Regular FTE Operating	500	0.8	375	1.0	500
Telephone Expenses	450	0.8	338	1.0	450
PC, One-Time	1,230	1.0	1,230		
Office Furniture, One-Time	3,473	1.0	3,473		
Subtotal Operating Expenses			**$ 5,416**		**$ 950**
TOTAL REQUEST		0.8	**$ 74,332**	1.0	**$ 92,018**
	General Fund:		*$ 74,332*		*$ 92,018*
	Cash funds:				
	Reappropriated Funds:				
	Federal Funds:				