

STATE OF COLORADO

OFFICE OF THE GOVERNOR

136 State Capitol
Denver, Colorado 80203
Phone (303) 866-2471
Fax (303) 866-2003



John W. Hickenlooper
Governor

D 2018-001

EXECUTIVE ORDER

Declaring a Disaster Emergency Due to the Colorado Department of Transportation (CDOT) Cybersecurity Incident in the State of Colorado, and Authorizing Deployment of the Colorado National Guard and Use of the Emergency Management Assistance Compact

Pursuant to the authority vested in the Governor of the State of Colorado and, in particular, pursuant to the Colorado Constitution, Article IV, Section 2, and pursuant to the relevant portions of the Colorado Disaster Emergency Act, C.R.S. § 24-33.5-701, *et seq.*, I, John W. Hickenlooper, Governor of the State of Colorado, hereby issue this Executive Order declaring a state of disaster emergency due to the CDOT Cybersecurity Incident in the State of Colorado, enabling state agencies to coordinate response efforts, and making resources available for response activities.

Further, pursuant to the Colorado Constitution, Article IV, Section 5, and pursuant to C.R.S. § 28-3-104, I also hereby authorize employing the Colorado National Guard for the purpose of responding to the CDOT Cybersecurity Incident in the State of Colorado.

Further, pursuant to C.R.S. § 24-60-2901 *et seq.*, I hereby authorize implementing the Emergency Management Assistance Compact, enabling access to additional resources outside of Colorado for response activities.

I. Background and Purpose

- a. The Governor is responsible for meeting the dangers to the state and people presented by disasters. The Colorado Disaster Emergency Act defines a disaster as “the occurrence or imminent threat of widespread or severe damage, injury, or loss of life or property resulting from any natural cause or cause of human origin.” C.R.S. § 24-33.5-703(3). The definition contemplates that a human-caused disaster may include a cybersecurity incident.
- b. According to an analysis of the incident, attempts to gain access to the CDOT network began on February 8, 2018 and access was gained on February 12, 2018. For the next nine days, the intruder(s) examined the network as well as attached

systems. Malicious software was installed on February 20, 2018, which activated the following day. The malicious software encrypted files on hundreds of computers throughout CDOT, and payment was demanded in order to receive instructions to decrypt the encrypted files. Upon discovery of the intrusion, CDOT employees were instructed to take immediate steps to minimize the impact of the malicious software. In addition to office computers, traffic metering systems were taken offline in CDOT Region 1, impacting traffic flows and safety, and potentially impeding emergency responses to all types of incidents, both on the highway system and those accessed by feeder roads. Over the ensuing days, CDOT and the Governor's Office of Information Technology (OIT) attempted to restore access to affected systems. As the incident progressed and additional cybersecurity issues were identified, OIT requested immediate assistance and expertise from cybersecurity specialists in the Colorado National Guard and the private sector. As part of the response to this incident, potential threats to the statewide network were identified, which raised further concerns for public safety.

- c. At approximately 1200 hours on March 1, 2018, I verbally declared a disaster emergency for the cybersecurity incident in the State of Colorado and activated the State of Colorado Hazard and Incident Response and Recovery Plan, also known as the State Emergency Operations Plan.
- d. I further verbally authorized deployment and use of the Colorado National Guard for the cybersecurity incident in the State of Colorado.

II. Declarations and Directives

- a. The CDOT Cybersecurity Incident and associated impacts constitute a disaster emergency under C.R.S. § 24-33.5-701, *et seq.* My verbal order of March 1, 2018, declaring a disaster emergency, is hereby memorialized by this Executive Order and shall have the full force and effect of law as if it were contained within this Executive Order.
- b. The State of Colorado Hazard and Incident Response and Recovery Plan, also known as the State Emergency Operations Plan, is hereby activated. All state departments and agencies shall take whatever actions may be required and requested by the Director of the Office of Emergency Management pursuant to the Emergency Support Function 5 Annex of the Colorado Hazard and Incident Response and Recovery Plan, including provision of appropriate staff and equipment as necessary.
- c. Due to the current insufficiency of funds necessary to pay for response efforts related to the CDOT Cybersecurity Incident in the Disaster Emergency Fund, I order the transfer of two million dollars (\$2,000,000) from the Controlled Maintenance Trust Fund into the Disaster Emergency Fund pursuant to C.R.S. § 24-33.5-706(4)(b). I further encumber two million dollars (\$2,000,000) in the Disaster Emergency Fund to pay for the response efforts related to the CDOT Cybersecurity Incident since February 21, 2018.

- d. Further, pursuant to C.R.S. § 24-33.5-705.4(5), the Director of the Office of Emergency Management is hereby authorized and directed to allocate the funding to the appropriate government agencies and non-profit organizations, and execute awards, purchase orders, or other mechanisms to effect the allocation of the funds. These funds shall remain available for this purpose until sixty (60) months from the date of this Executive Order, and any unexpended funds shall be reimbursed to accounts from which they were originally transferred.
- e. My verbal orders of March 1, 2018, activating the National Guard and authorizing the use of National Guard assets for the CDOT Cybersecurity Incident are hereby memorialized by this Executive Order and shall have the full force and effect of law as if they were contained within this Executive Order.

III. Duration

This Executive Order shall expire thirty (30) days from March 1, 2018, unless extended further by Executive Order, except that the funds described in paragraph II(c) above shall remain available for the described purposes for sixty (60) months from the date of this Executive Order.



GIVEN under my hand and
Executive Seal of the State of
Colorado this thirtieth day of March, 2018.

A handwritten signature in blue ink, appearing to read "John W. Hickenlooper", written over a horizontal line.

John W. Hickenlooper
Governor