

BEFORE THE NEW MEXICO
CHIEF INFORMATION SECURITY OFFICER

IN THE MATTER CONCERNING)
CYBERSECURITY INCIDENT REPORTING)
)
ORDER NO. 2025-01)
_____)

THIS MATTER comes before the New Mexico Chief Information Security Officer (“CISO”) *sua sponte*. The CISO, having considered the matter and being otherwise fully informed, issues an Order as follows:

WHEREAS:

1. Pursuant to Section 9-27A-3(A) of the New Mexico Cybersecurity Act, (Sections 9-27A-1 to 9-27A-5 NMSA 1978) (“Cybersecurity Act”), the New Mexico Legislature created the Office of Cybersecurity (“OCS”). The OCS is managed by the CISO.
2. Pursuant to Section 9-27A-3(B)(12) of the Cybersecurity Act, the OCS and the CISO may create a model cybersecurity incident response plan and establish a centralized cybersecurity and data breach reporting process for agencies and political subdivisions of the state.
3. Cybersecurity incidents may include unauthorized access of an information technology (IT) system, unauthorized access to or disclosure of electronic data, or the use of electronic processes, devices or communications to manipulate conduct of human actors. In an interconnected IT environment such as state government, any device, scheme or artifice that results in or risks disruption of an IT system or unauthorized access to digital information or that risks personal or economic injury to the state or any person is potentially repeatable, and therefore of interest to all agencies and political subdivisions of the state.
4. The Federal Information Security Modernization Act of 2014 (“FISMA”) defines a cybersecurity "incident" as an occurrence that:
 - A. actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
 - B. constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.”

5. The National Institute of Standards and Technology (“NIST”) promulgates standards for cybersecurity practices, including incident reporting and response. For large organizations, such as state government, NIST standards encourage centralized reporting and response.
6. NIST standards also recognize that timely notice of a cybersecurity incident, no matter the severity, to the entity responsible for prevention, mitigation and response to the incident facilitates risk and vulnerability assessment, promotes development and implementation of responsive actions for the impacted entity and all similarly situated entities, and facilitates incident mitigation and recovery.
7. Minimizing the dissemination of cybersecurity incident information through centralized reporting and management is a NIST recognized standard to avoid propagation of cybersecurity vulnerabilities and associated intrusions, and attempted intrusions.

WHEREFORE:

- A. It is in the best interest of New Mexico state government for the OCS and the CISO to receive prompt and exclusive notice of every cybersecurity incident experienced by agencies and political subdivisions of the state.
- B. The OCS and the CISO are authorized by statutory law to be the first and exclusive recipient of information concerning every cybersecurity incident experienced by agencies and political subdivisions of the state.
- C. It is in the best interest of New Mexico state government for the OCS and the CISO to determine when and who should receive notice of a cybersecurity incident.
- D. Having a single point of contact within state government for compliance with cybersecurity incident reporting requirements applicable to any agency or political subdivision of the state will promote compliance with those requirements and facilitate response coordination.
- E. Having a primary contact within each agency and political subdivision of the state responsible for providing notification of a cybersecurity incident and to serve as a liaison for incident response promotes compliance with notification requirements and facilitates response coordination with the OCS and the CISO.
- F. Having standardized policies and procedures for every agency and political subdivision of the state to follow when a cybersecurity incident occurs facilitates legal compliance, response, mitigation and recovery.

G. The definition of cybersecurity “incident” developed by FISMA is reasonable and instructive and should be adopted for purposes of this Order.

H. The CISO has jurisdiction and authority to issue an Order regarding cybersecurity incident reporting applicable to agencies and political subdivisions of the state.

NOW, THEREFORE, THE CISO HEREBY DIRECTS AS FOLLOWS:

1) The definition of cybersecurity “incident” developed by FISMA is hereby adopted for purposes of this Order.

2) Within 24 hours of discovering a cybersecurity incident involving the public entity or one of its vendors, an agency or political subdivision of the state shall notify and consult with the OCS.

3) The affected public entity shall notify and consult with the OCS prior to notifying or communicating with any other entity within or outside state government, unless the affected public entity is otherwise required by law or contract to directly notify or communicate with another outside entity, in which case the affected public entity shall simultaneously report the incident to the OCS and to that other entity. To the extent that a federal cybersecurity incident reporting requirement appears to conflict with this Order, the federal requirement and the requirements of this Order must be construed, if possible, to give effect to each. If the conflict is irreconcilable, the federal requirement shall control.

4) Any notification to OCS required by this Order shall be made by calling **(833) 42-CYBER (833-422-9237)**. A reporting entity shall provide the OCS representative with as much requested information as is available at the time of notification and shall update the notification as requested information becomes available.

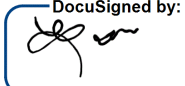
5) The OCS shall promptly triage the nature and severity of an incident and provide incident response coordination, assistance and support required by law, or as OCS deems appropriate, based on the OCS assessment. OCS shall promptly inform the affected agency of the incident coordination and response services that shall be performed by OCS, if any. Unless OCS directs otherwise after it completes incident triage, OCS shall exclusively make all required reports and serve as the point of contact ("POC") for federal or state response agencies.

6) An affected public entity shall ensure that support personnel remain available as directed by the OCS and shall ensure full cooperation of the support personnel with the OCS, the CISO, and any personnel involved in the analysis of, response to, and resolution of the incident.

7) Within 10 days of its receipt of this Order, each agency and political subdivision shall designate a POC in the form and manner specified by OCS. The designated POC shall report cybersecurity incident information to the OCS and the CISO and serve as a liaison between the OCS and the agency or political subdivision of the state for all cybersecurity incident investigation, mitigation and response. Any change in the identity of an agency POC shall be reported to the OCS within ten (10) days of the change in the same form and manner.

THIS ORDER is effective as of the date signed by the CISO and shall remain in effect until withdrawn or superseded by subsequent order. Pursuant to Section 9-27-5(E) of the Cybersecurity Act and Executive Order 2024-011, all public bodies, including non-executive agencies and tribal governments, are strongly encouraged to voluntarily comply with this Order.

DONE AND ORDERED THIS 30th DAY OF JUNE, 2025

BY:  437214FBE82C453...
RAJA SAMBANDAM
CHIEF INFORMATION SECURITY OFFICER