# Nev. Rev. Stat. Ann. § 480.900

This document is current through the end of legislation from the 82nd Regular Session (2023). This document incorporates revisions received from the Legislative Counsel Bureau for NRS Chapters 1 to 220. This document is current through the end of legislation from the 34th and 35th Special Sessions (2023), subject to revision by the Legislative Counsel Bureau.



## 480.900. Legislative findings and declarations regarding security of information systems.

The Legislature hereby finds and declares that:

**1.** The protection and security of information systems, and the coordination of efforts to promote the protection and security of information systems, are essential to protecting the health, safety and welfare of the people of this State.

**2.** The continued development of technologies relating to information systems and the expanding and diverse applications of those technologies pose significant implications for the functioning of any infrastructure in this State that is critical to the health, safety and welfare of the people of this State, particularly in the areas of transportation, health care, energy, education, law enforcement and commercial enterprises.

**3.** Information systems and the application of information systems relating to the operation of State Government and local governments make up a statewide cyberinfrastructure that is integral to the delivery of essential services to the people of this State and the essential functions of government that ensure the protection of the health, safety and welfare of the people of this State.

**4.** Protecting and securing the statewide cyberinfrastructure requires the identification of the areas in which information systems may be vulnerable to attack, unauthorized use or misuse or other dangerous, harmful or destructive acts.

**5.** Protecting and securing the statewide cyberinfrastructure requires an ability to identify and eliminate threats to information systems in both the public and private sectors.

**6.** Protecting and securing the statewide cyberinfrastructure requires a strategic statewide plan for responding to incidents in which information systems are compromised, breached or damaged, including, without limitation, actions taken to:

**(a)** Minimize the harmful impacts of such incidents on the health, safety and welfare of the people of this State;

**(b)** Minimize the disruptive effects of such incidents on the delivery of essential services to the people of this State and on the essential functions of government that ensure the protection of the health, safety and welfare of the people of this State; and

**(c)** Ensure the uninterrupted and continuous delivery of essential services to the people of this State and the uninterrupted and continuous operations of the essential functions of government that ensure the protection of the health, safety and welfare of the people of this State.

**7.** Protecting and securing the statewide cyberinfrastructure depends on collaboration and cooperation, including the voluntary sharing of information and analysis regarding cybersecurity threats, among local, state and federal agencies and across a broad spectrum of the public and private sectors.

**8.** Institutions of higher education play a critical role in protecting and securing statewide cyberinfrastructure by developing programs that support a skilled workforce, promote innovation and contribute to a more secure statewide cyberinfrastructure.

**9.** It is therefore in the public interest that the Legislature enact provisions to enable the State to prepare for and mitigate risks to, and otherwise protect, information systems and statewide cyberinfrastructure.

## History

2017, ch. 307, § 2, p. 1632, effective July 1, 2017.