New Mexico Department of Justice

February 3, 2026

OPINION
OF
RAÚL TORREZ
Attorney General

Opinion No. 2026-04

To: Representative Debra M. Sariñana

Re: Attorney General Opinion – Legislative Changes to Cybersecurity Act

---

Question

May the Legislature amend the Cybersecurity Act, NMSA 1978, §§ 9-27A-1 to -5 (2023), to provide the State Chief Information Security Officer (CISO) and the Cybersecurity Office the authority to set statewide cybersecurity standards and controls, and provide appropriate governance and application thereof, without violating the constitutional separation of powers? At a minimum, may the Legislature authorize the Cybersecurity Office and the CISO to specify minimum cybersecurity standards applicable to all connections to the state Information Technology (IT) network?

Short Answer

The Legislature may constitutionally delegate authority to the State CISO and Cybersecurity Office to set certain statewide cybersecurity standards and controls, depending on their substance. De minimis regulations do not violate the separation of powers. Regulations that do not conflict with express judicial rules and implicit core powers are permissible as well. Regulations that conflict, but do not substantially interfere with express judicial rules and implicit core powers might be constitutional. Regulations that unduly interfere with core judicial powers are not constitutional.

Background

New Mexico's Cybersecurity Office sits within the Department of Information Technology (DoIT) and is led by the State CISO. Sections 9-27A-3(A), -4. Under the Cybersecurity Act, the Office oversees cybersecurity and information security-related functions for executive agencies. Section 9-27A-2(A). Cybersecurity means "acts, practices or systems that eliminate or reduce the risk of loss of critical assets, loss of sensitive information or reputational harm as a result of a cyber attack or breach within an organization's network." Section 9-27A-2(B).

Analysis

The request asks whether proposed amendments to the Cybersecurity Act granting the State CISO and Cybersecurity Office rulemaking authority to set minimum cybersecurity standards would violate the separation of powers. Under the New Mexico Constitution, no branch "shall exercise any powers properly belonging to either of the others" except as expressly authorized in the Constitution. N.M. Const. art. III, § 1. There are two potential separation of powers issues. One, can the Legislature delegate rulemaking authority over cybersecurity standards to the State CISO and Cybersecurity Office? And two, does executive rulemaking authority over cybersecurity standards for the judicial branch infringe upon the separation of powers. We address each in turn.

1. Legislative Delegation of Authority

The Legislature can delegate rulemaking authority over cybersecurity standards to an executive agency like the Cybersecurity Office. Courts analyze the separation of powers issue in legislative delegations of authority under the nondelegation doctrine. A creature of the New Mexico Constitution, "[t]he nondelegation doctrine limits, but does not completely prevent, the Legislature from vesting a large measure of discretionary authority in administrative officers and bodies." *Cobb v. State Canvassing Bd.*, 2006-NMSC-034, ¶ 41, 140 N.M. 77.

The Legislature cannot delegate "unbridled or arbitrary" authority to the executive. *Id.* But if the Legislature dictates "reasonable standards" with specificity proportional to the scope of delegated authority, the delegation is constitutionally permissible. *Id.*; *compare Montoya v. O'Toole*, 1980-NMSC-045, ¶¶ 4–5, 94 N.M. 303 (upholding a statute containing "specific legislative standards" with specific factors and thresholds), *with Cobb*, 2006-NMSC-034, ¶¶ 15–16 (holding the Legislature cannot delegate "unfettered discretion" with no standards); *see also Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 474 (2001) (observing that "[i]n the history of the [United States Supreme] Court . . . only two statutes" had ever been struck down on nondelegation principles).

In short, most delegations of power from the Legislature to the executive branch are constitutional, as long as the Legislature prescribes standards for the exercise of delegated authority and sets limits on the same. This analysis applies in equal force to the authority of the Cybersecurity Office and State CISO to set cybersecurity standards. Accordingly, as long as the Legislature includes specific language guiding and limiting the delegated authority, the delegation is likely constitutional.[1]

2. Regulation of Judicial Branch

Whether the Legislature can delegate authority to the executive branch to set cybersecurity standards that apply to the judicial branch is a more difficult question. Nonetheless, we find the

[1] If there is concern about foreclosing the ability of other executive branch agencies to set standards that go beyond, but are consistent with, the minimum standards, statutory or regulatory language explaining that the State CISO and Cybersecurity Office standards are meant as a baseline would likely accomplish that effect.

Legislature likely has authority to set such minimum standards vis-à-vis a delegation to the executive so long as they do not infringe on the core powers of the judiciary.
We will assume, based on the request, in reading the phrases "statewide" or "all connections to the state IT network" in conjunction with the stated concern about separation of powers, that there is concern about how and whether the Cybersecurity Office and State CISO can, consistent with the New Mexico Constitution, regulate the *judicial branch's* information technology infrastructure. As currently written, the Cybersecurity Act only authorizes the Cybersecurity Office and State CISO to regulate "executive cabinet agencies and their administratively attached agencies, offices, boards and commissions." Sections 9-27A-2(A), -3(B).[2]

We will break this separation of powers doctrine question down into two parts. First, can the Cybersecurity Office and State CISO *condition* the voluntary use of agency-operated or -owned networks by the judicial and legislative branches? And second, if the judicial and legislative branches are not using agency-operated or -owned networks, can the Cybersecurity Office and State CISO still set minimum standards for those networks?

a. Conditioning Use of Executive Branch Networks

The separation of powers doctrine is not "absolute," and the Supreme Court has recognized that there must be some "overlap" among the branches. *State ex rel. Clark v. Johnson*, 1995-NMSC-048, ¶ 32, 120 N.M. 562 (citation modified). The central inquiry is whether one branch "unduly interferes with or encroaches on the authority or within the province of a coordinate branch of government." *State ex rel. Candelaria v. Grisham*, 2023- NMSC-031, ¶ 14 (citation modified). An unlawful disruption of the balance must amount to "more than de minimis dissonance or conflict." *Amdor v. Grisham*, 2025-NMSC-024, ¶ 113.

In accordance with these principles, the answer to the first question is yes—the Cybersecurity Office and State CISO may condition the judicial branch's general use of agency-operated or -owned telecommunications networks on certain minimum cybersecurity standards. At the outset, we note the Cybersecurity Act already appears to delegate some of that authority. Section 9-27A-3(B)(2) grants the Office the power to "develop minimum cybersecurity controls . . . for *all entities* that are connected to an agency-operated or -owned telecommunications network." (Emphasis added); 1.12.20.2 NMAC (applying DoIT regulations "to all executive branch agencies, and any other state entity which utilizes the state information technology (IT) infrastructure"). The Act also authorizes the DoIT to "enter into necessary agreements to provide, where feasible, a telecommunication network and related facilities to all executive, legislative and judicial branches." Section 9-27-20(A).

---

[2] We also note that the Cybersecurity Act neither creates nor regulates a singular "state network" or "state IT network" as described in your request. Instead, the Act regulates a universe of "products and services" used by state agencies, and discusses "agency-operated or -owned telecommunications network[s]." Section 9-27A-2(D) (defining "information technology"), § 9-27A-3(B)(2); *see also* Fiscal Impact Report for S.B. 129, 56th Leg., 2nd Sess., at 4 (N.M. 2024) (noting that "[a]lthough some of New Mexico's cybersecurity operations and policies are housed within DoIT, state cyber operations are siloed in different agencies").

To answer this question it is helpful to rephrase it: Is there anything in New Mexico's separation of powers caselaw that compels the executive branch (acting pursuant to legislatively delegated authority) to provide some constitutional minimum telecommunications infrastructure to the other branches? If no such constitutional mandate exists, then the executive branch would be entitled to condition judicial and legislative branch access to its networks like any other service provider and negotiate the terms of providing those services. In effect, the judicial branch would then be faced with a choice of using the executive branch systems (with conditions) or seeking alternatives.

Neither the executive nor legislative branch is constitutionally required to host such a network. While the issue has not been squarely raised in New Mexico, our Supreme Court has implied, and other states have held, that legislatures have a legal duty to appropriate money for the adequate functioning of courts. *See Mowrer v. Rusk*, 1980-NMSC-113, ¶ 29, 95 N.M. 48 (suggesting courts "may incur necessary and reasonable expenses in the performance of their judicial duties" (quoting *Smith v. Miller*, 384 P.2d 738, 741 (Colo. 1963))); *see also State ex rel. J.C. v. Mazzone*, 759 S.E.2d 200, 209 (W. Va. 2014) ("Courts have inherent authority to require necessary resources, such as sufficient funds for operating expenses, work space, parking space, supplies, and other material items." (citation modified)). These resources must be "reasonably necessary for the performance of [the courts'] responsibilities in the administration of justice." *J.C.*, 759 S.E.2d at 209 (citation modified). But nothing in this duty requires that the executive branch *host* the cybersecurity infrastructure of the courts—the duty only requires that the judicial branch have sufficient resources to carry out its cybersecurity operations.

Thus, there is no violation of the separation of powers doctrine if the executive branch were to impose conditions on the judicial branch's connection to executive branch-owned or -operated networks in compliance with certain minimum cybersecurity standards.[3]

b. Regulating Networks Operated Independently by the Judicial Branch

The second question—whether the State CISO and Cybersecurity Office can promulgate rules that govern a network owned and operated entirely by the judicial branch (i.e. not an "agency network")—is a somewhat closer call. In sum, we find that where the standards pose de minimis requirements on the judicial branch, they are permissible. Where the standards are more than de minimis, the standards will govern (1) in the absence of conflicting judiciary policy and (2) so long as they do not substantially interfere with the core functions of the judicial branch.

In answering this question, we first note that there is nothing inherently improper about the Legislature delegating *authority* to the Cybersecurity Office and State CISO to set rules for the judiciary. Whether any regulations promulgated pursuant to this authority violate the separation of powers doctrine, however, will depend on the specific requirements they impose on the judiciary. In other words, the proposed amendment is not unconstitutional, but the regulations might be.

---

[3] This conclusion notwithstanding, the judiciary may itself be prohibited from agreeing to such conditions if those minimum standards, in the judiciary's view, violate the separation of powers, because separation of powers issues are generally not considered waivable. *Freytag v. Comm'r of Internal Revenue*, 501 U.S. 868, 880 (1991).

i. Separation of Powers in New Mexico

Separation of powers issues fall between two poles: de minimis conflicts and undue interference. A de minimis regulation of another branch does not threaten the separation of powers. While our Supreme Court has not defined precisely what constitutes a de minimis regulation, *Amdor v. Grisham*, 2025-NMSC-024, ¶ 113, certain ministerial duties imposed on the judiciary—e.g., the responsibility to submit "a report of the activities of the administrative office of the courts and of the state of business of the courts"—are likely de minimis. NMSA 1978, § 34-9-3(C) (2019).

At the other end of the spectrum, a regulation that "unduly interferes" with the core judicial power is never permissible. *Clark*, 1995-NMSC-048, ¶ 32. Whether a regulation unduly interferes with the powers of another branch requires a more complex analysis. While each branch possesses inherent powers, some powers are shared and others are exclusive. If a power is exclusive, like the judiciary's power to "directly control court personnel" and their hiring and firing, the Legislature has no authority to regulate the issue because it would substantially interfere with the judicial branch's core functions. *Mowrer v. Rusk*, 1980-NMSC-113, ¶ 31, 95 N.M. 48.

If a power is shared, the question requires a more complex inquiry. *Sw. Cmty. Health Servs. v. Smith* (*SCHS*), 1988-NMSC-035, ¶ 6, 107 N.M. 196. Where a power is shared, the first question is whether there is a true conflict between its exercise by two coordinate branches. *Id.* ¶ 12; *Pena v. State*, 2025-NMSC-041, ¶ 17. A statute can conflict with either an express judicial rule or a core judicial function. *Id.* ¶¶ 8, 15, 20. If there is no conflict with either, the exercise is permissible. *State v. Rivera*, 2012-NMSC-003, ¶ 8. If there is a conflict, "[w]hich branch must yield to the other depends upon the circumstances of each individual case" and the "essence of power exercised by the other branch of government." *SCHS*, 1988-NMSC-035, ¶¶ 12, 15; *see Padilla v. Torres*, 2024-NMSC-007, ¶¶ 26, 27. The relevant question is whether the statute "unduly interferes" with the judicial rule or power. *Clark*, 1995-NMSC-048, ¶ 32.

In this case, judicial administration appears to be a shared power, as the Legislature appropriates funding to the courts, "make[s] public policy," and passes laws that govern the administrative structure of the judicial branch. *Torres v. State*, 1995-NMSC-025, ¶ 10, 119 N.M. 609; *see Flynn v. Dep't of Admin.*, 576 N.W.2d 245, 257 (Wis. 1998) (in state where supreme court enjoys similar power of superintending control, judicial funding is area of shared authority); *e.g.* NMSA 1978, § 34-9-1 (1959) (setting up the Administrative Office of the Courts). Whether the judicial or legislative branch must yield will likely depend on the regulation and to what extent it impacts the core functions of the judicial branch. *See, e.g.*, *Flynn*, 576 N.W.2d at 257–58 (reduction in funding for court automation permissible because it did not "unreasonably curtail the powers or materially impair the efficacy of the courts or judicial funding" and mere "adverse impact" on court function insufficient to find separation of powers violation).

In sum, de minimis regulations of the judicial branch are permissible. Judicial administration is likely a shared power, so cybersecurity regulations that do not conflict with express judicial rules or implicit judicial powers are probably valid. If cybersecurity regulations conflict with a judicial rule or power, they may be invalid, depending on whether that conflict unduly interferes with the judicial branch's powers.

ii. Cybersecurity regulation

We now turn specifically to the legislative amendment suggested in the request. The request references concerns raised by the Administrative Office of the Courts (AOC) when similar legislation was previously introduced.[4] Then, the AOC expressed concern that the legislation would "allow the cybersecurity office to monitor and audit judicial networks and systems." Fiscal Impact Report for S.B. 129, 56th Leg., 2nd Sess., at 4 (N.M. 2024). On the one hand, we agree with the AOC that allowing unfettered access by the executive branch to judicial networks, even for the sole purpose of monitoring and auditing such systems, would likely run afoul of the separation of powers because confidentiality is a prerequisite to the effective exercise of the judiciary's core powers. [5] *See Pacheco v. Hudson*, 2018-NMSC-022, ¶¶ 43–51 (finding that a judge's emails stored on "computer servers of JID, a statewide entity operating under the supervision of the Administrative Office of the Courts" were not subject to disclosure under IPRA due to judicial deliberations privilege). On the other hand, imposing certain basic cybersecurity requirements (e.g., two-factor authentication, password complexity) would likely not infringe on core judicial powers and falls somewhere between a de minimis requirement and one that could be imposed absent conflicting judiciary policy.[6] Ultimately, the separation of powers issue will turn on the proposed substance of the regulation.

The above analysis primarily concerns direct regulation of the judiciary's cybersecurity by the legislative and executive branches. In other words, can the judiciary's own systems be bound by standards it did not itself promulgate? However, the separation of powers question is somewhat easier where the legislature requires the judiciary to adopt standards but leaves ultimate control over those standards to the judicial branch. Our statutes contain many similar provisions that, so far, remain unchallenged. *See, e.g.*, NMSA 1978, § 34-1-11 (2009) (authorizing the Supreme Court

---

[4] Though we refer to comments made about the previous legislation referenced in the request, this opinion should not be interpreted as opining on the constitutionality of that legislation generally or any specific provision, only the specific amendments discussed in the request.

[5] The request raises the example of the state's General Services Department, which is tasked with maintaining physical facilities of the state, including some for the court system (e.g., the offices of the Administrative Office of the Courts). Using that analogy, we could imagine that a regulation requiring court offices comply with certain safety requirements (e.g., a minimum number of fire exits) would probably not run afoul of the separation of powers. On the other hand, a regulation requiring security cameras in rooms where sensitive decisions are made, monitored by an executive branch agency, might infringe on the confidentiality of the judiciary and run afoul of the separation of powers.

[6] Currently, the Legislature has provided for judicial branch management of "all matters relating to administration of the courts" by the AOC, including the Judicial Information Division (JID), "the technology arm of the New Mexico Judiciary, providing cybersecurity and technical support to all state courts, including email, network access, and the Odyssey electronic case management system." NMSA 1978, § 34-9-3(A) (2019); New Mexico Judiciary, *Annual Report 2024*, at 33, https://nmcourts.gov/new-mexico-judiciary-annual-report-2024/. The judicial branch has also established for itself a Judicial Technology Council (JTech). *See* Order, *In the Matter of the Renaming of the Judicial Technology Committee and the Appointment of Members*, S-1-AO-2023-00009 (Jun. 27, 2023). It is unclear what standards these bodies have adopted.

to impose electronic services fee); NMSA 1978, § 34-2-11 (2018) (establishing the Supreme Court Law Library and vesting its management in the Supreme Court).

Requiring the judiciary to set cybersecurity standards without specifically dictating the actual substance of those standards is unlikely to pose a separation of powers concern. *See, e.g.*, *Padilla*, 2024-NMSC-007, ¶ 29 (citing with approval NMSA 1978, § 34-8A-6(A) (2019), which "instructs" Supreme Court to "'adopt separate rules of procedure for the metropolitan court'"); *see also Saltonstall v. City of Sacramento*, 231 Cal. App. 4th 837, 855 (2014) ("The Legislature may direct the Judicial Council to adopt rules of court to implement statutes that do not defeat or materially impair a court's exercise of its constitutional power or the fulfillment of its constitutional function." (citation modified)); Kan. Stat. Ann. § 75-7206 (2026) (establishing Judicial Chief Information Officer under the supervision of judicial administrator and chief justice with authority over judicial cybersecurity standards). In other words, requiring the judiciary to develop its own cybersecurity standards likely does not violate the separation of powers. Or, to provide another example, requiring the judiciary to conduct *its own audit* of its cybersecurity systems is unlikely to flout the separation of powers.

Conclusion

For the reasons outlined above, we conclude that the amendment proposed in the request is likely constitutional. However, any regulations promulgated pursuant to that authority may be unconstitutional if they unduly interfere with the judiciary's core powers.

* * *

Please note that this opinion is a public document and is not protected by the attorney-client privilege. It will be published on our website and made available to the general public.

RAÚL TORREZ
ATTORNEY GENERAL