LFC Requester:	

AGENCY BILL ANALYSIS
2026 REGULAR SESSION

WITHIN 24 HOURS OF BILL POSTING, UPLOAD ANALYSIS TO:

AgencyAnalysis.nmlegis.gov

{Analysis must be uploaded as a PDF}

SECTION I: GENERAL INFORMATION
{Indicate if analysis is on an original bill, amendment, substitute or a correction of a previous bill}

Check all that apply:
Original x **Amendment** ___
Correction ___ **Substitute** ___

Date 1/20/2026
Bill No: HB 46-280

Sponsor: Kathleen Cates
Short Title: Crime of Digital Sabotage of a Business

Agency Name and Code Number: LOPD-280
Person Writing Tania Shahani
Phone: 505 395 2890 **Email** Tania.Shahani@lopdnm.us

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY25	**FY26**		

(Parenthesis ( ) Indicate Expenditure Decreases)

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY25	**FY26**	**FY27**		

(Parenthesis ( ) Indicate Expenditure Decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY25	FY26	FY27	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total						

(Parenthesis ( ) Indicate Expenditure Decreases)

Duplicates/Conflicts with/Companion to/Relates to:
Duplicates/Relates to Appropriation in the General Appropriation Act

SECTION III: NARRATIVE

BILL SUMMARY

Synopsis:

HB 46 amends the Computer Crimes Act (NMSA 1978, Sec. 30-45-1, et. seq) definitions and creates a new crime with corresponding penalties for "digital sabotage of a business."

Section 1 would define the terms "digital resource" (including a computer, system, network, domain name system, or software application) and defines **"**domain name system.**"**

Section 2 would create a new offense, Section 30-45-3.1, digital sabotage of a business. The new offense would punish conduct directed at a business's "digital resource." The person who would commit the crime must knowingly and willfully, and without the business's authorization, use or modify a digital resource used by the business in a way that either (1) diverts someone searching for the business to a different network location, (2) impairs or damages the digital resource's functioning or the business's operations, or (3) harms the business's reputation by supplying false or misleading information through that digital resource.

The penalty structure would be based on "damage caused." The bill grades the offense from petty misdemeanor to second-degree felony depending on the dollar amount of damage, and adds a recidivist felony provision for repeated low-damage offenses.

FISCAL IMPLICATIONS

LOPD does not anticipate a significant increase in prosecutions as a result of adding this offense to the Computer Crimes Act, and therefore expects little immediate fiscal impact. However, Section 30-45-3.1 authorizes felony grading up to a second-degree felony based on the amount of alleged "damage," which may result in more felony filings in some cases. These cases may also require specialized digital-forensics expertise, increasing the cost and complexity of defense.

LOPD may be able to absorb some additional workload associated with this proposal. But even incremental increases—when combined with the cumulative effect of other criminal legislation—create a corresponding need for additional indigent defense resources to ensure continued compliance with constitutional mandates.

Absent some offsetting reduction in indigent defense workload, any increase in felony

prosecutions would likely require additional indigent defense funding to prevent existing capacity constraints from worsening. The precise fiscal impact cannot be predicted in advance; the need for resources would have to be evaluated after implementation and based on actual charging and litigation patterns. Given current budget limitations, LOPD remains concerned about the cumulative effect of new offenses and enhanced penalties on overall caseloads and system strain.

SIGNIFICANT ISSUES

There seems to be redundancy with HB 46 and crimes already contained in the Computer Crimes Act. To the extent the intent of HB 46 is to target account takeovers, DNS hijacking, or other direct interference with a business's digital assets, the proposed language fails to track that conduct precisely, which may increase interpretive disputes and overbreadth concerns.

Generally, to incur criminal liability, New Mexico law requires a minimum mental state of recklessness (i.e., conscious disregard of the risk of harm). *See State v. Yarborough*, 1996-NMSC-068, ¶ 13, 122 N.M. 596 ("Ordinary negligence, not amounting to willful or wanton disregard of consequences, cannot be made the basis of a criminal action.") While this bill requires a person act knowingly and willfully, it is unclear whether the knowledge or willful requirement attaches to the underlying *conduct* or with respect to the resulting *damage*. To justify criminal, rather than civil, liability, Analyst recommends incorporating a requirement that the person acted either intending the resulting damage or with conscious disregard of the risk of such damage.

The new, business-focused offense created (§ 30-45-3.1) arises in a statutory area where existing provisions already sweep pretty broadly. In particular, § 30-45-5 (unauthorized computer use) is drafted in unusually dense and expansive terms. It pairs alternative authorization theories ("without authorization" or "having obtained authorization" but using it for purposes beyond its scope) with a sweeping list of covered conduct ("accesses, uses, takes, transfers, conceals, obtains, copies or retains possession") and an equally broad list of covered items ("computer…network…property…service…system"). That structure is difficult to parse and risks inconsistent interpretations about what conduct is actually prohibited.

This seems especially so in cases turning on whether a person merely violated a use policy or instead bypassed some kind of restriction to access. Against that backdrop, much of the conduct HB 46 targets, like interfering with a business's online functioning, diverting users, or manipulating information in a way that harms operations, may already be chargeable under §§ 30-45-4 and 30-45-5 depending on the factual scenario presented. The addition of § 30-45-3.1 therefore may not fill a clear gap so much as add another overlapping theory of liability, increasing prosecutorial discretion and the risk of charge-stacking or charge inflation, while also compounding litigation over two recurring ambiguities: what counts as "authorization" (or "exceeding authorization") in common online contexts, and how "damage" is calculated—particularly where asserted losses are reputational or otherwise difficult to quantify.

The "reputation prong" may be overly broad and subject to arbitrary application in a criminal context, as it could apply to a sweeping range of conduct. If the legislative objective is to address account takeovers, hijacking, or unauthorized edits, the current "reputation" formulation is not well-tailored to that problem and may sweep more broadly than necessary. As proposed, the bill would be criminalizing conduct that harms a business's reputation by providing "false or

misleading information." That is written broadly enough to risk encroaching on First Amendment protections, particularly in cases involving online criticism or consumer disputes rather than true digital interference. The problem is compounded by the bill's penalty scheme because the offense level turns on the dollar value of "damage," and measuring reputational harm invites inflated or speculative valuation creating a significant risk of increasing the level of felony based on contestable harms and soft numbers.

Relatedly, the bill's authorization element ("without authorization of a business") may be unclear in common online settings where platforms permit third-party edits or user-generated content about a business. Since the statute turns on the business's authorization, litigation may focus on what counts as "authorization," and whether publicly available interactions with a platform constitute "using" a "digital resource used by" the business.

Also worth noting is that New Mexico's existing criminal libel statute, 30-11-1, also targets publishing or circulating false and malicious statements affecting another's reputation or business (as a misdemeanor). HB 46 narrows the context to certain digital resources but layers on felony gradations tied to "damage," potentially creating interpretive and charging questions about when prosecutors should proceed under § 30-45-3.1 versus existing reputation-based offenses.

PERFORMANCE IMPLICATIONS

ADMINISTRATIVE IMPLICATIONS

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

TECHNICAL ISSUES

Analyst is unaware whether this legislation is germane under Art. IV, Section 5. It is not a budget bill and analyst is unaware that it has been drawn pursuant to a special message of the Governor.

OTHER SUBSTANTIVE ISSUES

ALTERNATIVES

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

AMENDMENTS