FISCAL IMPACT REPORT

		LAST UPDATED	
SPONSOR	Dixon/Serrato/Ortiz y Pino/Maestas	**ORIGINAL DATE**	2/21/2023
		BILL	
SHORT TITLE	Technology Sandbox Act	**NUMBER**	House Bill 356
		ANALYST	Gray

APPROPRIATION*
(dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY23	**FY24**		
	$400.0	Recurring	General fund

Parentheses ( ) indicate expenditure decreases.
*Amounts reflect most recent analysis of this legislation.

Sources of Information

LFC Files

Responses Received From
New Mexico Attorney General (NMAG)
Economic Development Department (EDD)
Regulation and Licensing Department (RLD)
Department of Information Technology (DoIT)

SUMMARY

Synopsis of House Bill 356

House Bill 356 appropriates $400 thousand from the general fund to the Office of Attorney General (NMAG) to fund staff that will administer the Technology Sandbox Act.

HB356 creates the Technology Sandbox Act to provide temporary licensing waivers for individuals and businesses that propose an innovative use of blockchain technology. The bill requires that applicants submit an application including a description of the service, consumer risks, a business plan, and the expertise of the applicant among other information. HB356 requires the NMAG to evaluate the risk of any entity receiving a regulatory waiver, and the bill also requires a participant to post a consumer protection bond as security for potential losses and damages suffered by consumers.

The bill requires NMAG to publish rules of enforcement and implementation of the act.

This bill does not contain an effective date and, as a result, would go into effect June 16, 2023, (90 days after the Legislature adjourns) if signed into law.

FISCAL IMPLICATIONS

The appropriation of $400 thousand contained in this bill is a recurring expense to the general fund. Any unexpended or unencumbered balance remaining at the end of FY24 shall revert to the general fund.

NMAG analysis notes that HB356 will have on-going recurring costs, though the bill provides an appropriation for one fiscal year. NMAG notes that the agency will require at least one highly qualified and specialized staff to review applications in the agency, with Department of Information Technology (DoIT) staff, attorneys, and others.

Analysis from the Economic Development Department (EDD) notes the bill may result in some additional economic development opportunities, expand businesses, create jobs, and contribute to innovation. These may increase the tax base and promote revenues.

However, other state's experience with regulatory sandboxes have yielded mixed results. For example, Arizona passed an initiative in early 2019 that sought to decrease the burden on innovative financial products of services. However, news reports have identified that only 13 companies have filed an application under that program. The scope of HB356 is smaller than the program enacted in Arizona, so it is unlikely that HB356 will increase tax revenue directly.

SIGNIFICANT ISSUES

Background. The first formal regulatory sandbox is attributed to the UK Financial Conduct Authority (FCA), defined as a "safe space" for businesses to "test innovate products, services, business models and delivery mechanisms" without immediately incurring regulatory costs. In the U.S., several federal regulatory agencies have set up sandbox policies, and many states–including Arizona, Wyoming, Utah, and Ohio–have embraced such policies.

Notably, in 2019, a number of state Attorneys General urged the Consumer Financial Protection Bureau (CFPB) to oppose sandbox policies, and CFPB terminated two of its sandbox programs in September 2022. Sandbox programs are not without risk, and implementing a program to address blockchain technology may present challenges.

Security risks. Analysis from DoIT notes that blockchain security risks and operational functions requires a high degree of specialization and that blockchain specialists are typically highly compensated. This may present challenges for NMAG to hire the staff needed to establish sufficient criteria and safeguards that protect residents and institutions from risks related to a compromise of blockchain technology.

Legal concerns. Analysis from several agencies note that HB356 may result in legal concerns, including litigation, separation of powers issues, and constitutional conflicts.

For example, HB356 provides that the decision from NMAG will not be subject to judicial review. NMAG analysis notes:

> This provision could be challenged in court, which have previously ruled that, "The reviewability of executive and legislative acts [by the judicial branch] is implicit and inherent in the common law and the division of powers between the three branches of

government. . . . We have subject matter jurisdiction to review all executive and legislative acts." *State ex rel. Village of los Ranchos de Albuquerque v. City of Albuquerque*, 1994-NMSC-126, ¶ 15. Decisions instead could be subject to discretionary review under Rule 1-075 NMRA.

The bill also requires NMAG to coordinate with the agency which issues a license for which a waiver is requested. NMAG analysis notes that New Mexico has a divided executive branch consisting of the governor and many executive entities, including the Attorney General. Each executive entity is empowered by separate statutes. NMAG analysis writes:

A statute requiring that an entity under the control of one executive office must "coordinate" with an entity under the control of a different executive office, should either clearly direct all involved agencies to "coordinate," or grant authority to an executive office to direct the actions of agencies ordinarily under the control of a different executive agency when necessary to effectuate the goals of the empowering statute.

DoIT analysis notes that authorizing NMAG to grant regulator waivers present concerns because providing those may be considered creating special laws, a violation of the separation of powers and a delegation of legislative authority.

Analysis from Regulation and Licensing Department (RLD) writes that sandbox participants should:

…be encouraged to comply with existing consumer protection and disclosure laws and, if needed, engagement with regulators on requests for limited relief. For example, a description of the securities being offered should be provided along with a disclosure document clearly describing describe how the Interest Accounts operate and the general terms of the investment. This includes describing how interest will be computed or accrue, when and how the sandbox participant will pay interest to the investor, the deposit terms, the investors' rights to withdrawal, and the types of digital assets that may be deposited.

RLD also notes that the Federal Deposit Insurance Corporation (FDIC) has ordered multiple blockchain companies to cease-and-desist making false representations. The FDIC later issued a board warning to the cryptotechnology industry noting that federal deposit insurance extends to banks but not to crypto companies.

Economic development. Analysis from EDD notes that HB356 may make launching a blockchain startup and doing business in New Mexico more attractive. However, the analysis notes that provisions that require applications to be public may prevent some applicant participation. New blockchain technology applications are likely highly proprietary and businesses may hesitate to release that information publicly, EDD analysis writes. Similarly, EDD analysis notes the requirement that the consumer bond be in place for two years may be cost prohibitive.

Cyber risks. DoIT analysis notes that blockchain technologies have cybersecurity risks that could undermine uses. The analysis writes:

Cyber risks for blockchain technologies are listed below and could potentially undermine the use cases:

- **Routing attacks.** Blockchains depend on immense data transfers performed in real-time. Resourceful hackers can intercept the data on its way to ISPs (Internet Service Providers). Unfortunately, blockchain users don't notice anything amiss.
- **51% attacks**. Large-scale public blockchains use a massive amount of computing power to perform mining. However, a group of unethical miners can seize control over a ledger if they can bring together enough resources to acquire more than 50% of a blockchain network's mining power. Private blockchains aren't susceptible to 51% attacks, however.
- **Sybil attacks**. Named for the book that deals with multiple personality disorder, Sybil attacks flood the target network with an overwhelming number of false identities, crashing the system.
- **Phishing attacks.** This classic hacker tactic works with blockchain as well. Phishing is a scam wherein cyber-criminals send false but convincing-looking emails to wallet owners, asking for their credentials.

TECHNICAL ISSUES

HB356 does not provide an expansive definition of blockchain technology. Many items can be traded on the blockchain, including digital coin assets or crypto currency assets. HB356 defines "blockchain technology" as "the use of a digital database containing records of transactions, which can be simultaneously used and shared within a decentralized, publicly accessible network and can record transactions between two or more parties in a verifiable and permanent way."

In contrast, the U.S. Securities and Exchange Commission (SEC) defines the blockchain (in relation to the change of digital assets) as "a decentralized ledger maintained by a network of independently owned computers. New data is connected to previous blocks, forming a chain. Digital tokens are used to compensate 'miners' who validate transactions and allow for peer to peer 'transfers of value,' which are then logged in the decentralized ledger." *SEC v. LBRY, Inc*. Case No. 21-cv-260-PB, Opinion No. 2022 DNH 138.

BG/ne/rl