FISCAL IMPACT REPORT

SPONSOR SFC **LAST UPDATED** 03/17/23
ORIGINAL DATE 03/01/23
BILL NUMBER CS/CS/Senate Bill 280/SRCS/SFCS/aSFl#1 /aHAFC

SHORT TITLE Cybersecurity Act

ANALYST Hitzman

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT*
(dollars in thousands)

	FY23	FY24	FY25	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Agency DoIT Fees	Indeterminate but substantial	Indeterminate but substantial	Indeterminate but substantial		Recurring	General Fund
Council Per Diem	~$15.8	~$15.8	~$15.8	~$47.4	Recurring	General Fund
DoIT Operating Budget	($1,200.0)	($5,200.0)	NFI	($6,400.0)	Nonrecurring	General Fund
Office Operating Budget - *Projected*	1,200.0	8,800.0	10,000.0	20,000.0	Recurring	General Fund
Total	~$26.0	~$3,626.0	~$10,026.0	~$13,078.0		

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

Relates to Senate Bill 269.
Relates to an appropriation in the General Appropriations Act.

Sources of Information

LFC Files
National Conference of State Legislatures (NCSL)
National Association of State Chief Information Security Officers (NASCIO)
U.S Department of Homeland Security

Responses for Original Bill Received From
Department of Finance and Administration (DFA)
Office of Attorney General (NMAG)
Administrative Office of the Courts (AOC)
Department of Information Technology (DoIT)

SUMMARY

Synopsis of HAFC Amendments to Senate Bill 280

House Appropriations and Finance Committee amendments to Senate Bill 280 (SB280) remove the appropriation.

Synopsis of SFl#1 Amendment for Senate Bill 280

The Senate Floor amendments to Senate Bill 280 specify that the three members of the cybersecurity advisory committee representing counties shall be appointed by the chair of the board of directors of the New Mexico association of counties and the three members who represent municipalities shall be appointed by the chair of the board of directors of the New Mexico municipal league, rather than appointed by the security officer.

Synopsis of SFC Substitute for Senate Bill 280

The Senate Finance Committee substitute for Senate Bill 280 (SB280) creates the Cybersecurity Act, provides definitions, and adds user and system credentials to the definition of "information technology." The bill creates the Cybersecurity Office, administratively attached to the Department of Information Technology (DoIT) and managed by the state chief information security officer. The office shall oversee cybersecurity- and information-security-related functions for agencies except as required by federal law. The office may be responsible for:

1) Adopting and implementing rules to establish minimum security standards and policies to protect agency information technology (IT) systems and infrastructure, provide appropriate governance and application of the standards and policies and promote the availability, confidentiality and integrity of the information processed, transacted or stored by the state's IT infrastructure and systems;
2) Develop minimum cybersecurity controls for managing and protecting information technology assets and infrastructure for all entities that are connected to an agency-operated or -owned telecommunications network;
3) Monitor agency IT networks, consistent with information security standards, to detect incidents and support mitigation efforts as necessary and within capabilities; Access information technology systems connected to agency-operated or -owned telecommunications networks as reasonably necessary for detection and monitoring;
4) As reasonably necessary, obtain agency system event logs to support monitoring and detection;
5) In coordination with state and federal cybersecurity emergency management agencies, create a model incident-response plan for public bodies to adopt with the cybersecurity office as the incident-response coordinator for certain types of incidents;
6) Serve as a cybersecurity resource for local governments;
7) Develop a service catalog of cybersecurity services to be offered to agencies and to political subdivisions;
8) Collaborate with agencies in developing standards, functions and services;
9) Establish core services to support minimum security standards and policies;
10) Establish minimum data classification policies and standards and design controls for compliance;
11) Develop and issue cybersecurity awareness policies and training standards and offer cybersecurity training services; and
12) Establish a centralized cybersecurity and data breach reporting process for agencies and political subdivisions of the state.

The bill creates the position of state chief information security officer, who shall be a classified position in accordance with the Personnel Act. The bill also creates the cybersecurity advisory council within the cybersecurity office to assist in the development of a statewide cybersecurity plan, guidelines for best cybersecurity practices for agencies, and recommendations for remediation actions, and the committee will have the authority over hiring, supervision, discipline, and compensation of the security officer. The security office or designee will chair the committee with representation from the Administrative Office of the Courts or designee, the Legislative Council Service director or designee, tribal governments, county governments (three members), municipal governments (three members), and designees of other departments with cybersecurity experience to be appointed by the governor (three members). The cybersecurity advisory committee may form subcommittees to address specific or regional cybersecurity issues as it deems necessary and may invite other representatives as determined necessary.

The meetings of and materials presented to or generated by the cybersecurity advisory committee are subject to the Open Meetings Act and Inspection of Public Records Act (IPRA), unless under exceptions where the meeting or material could expose a vulnerability in a public IT system or a cybersecurity solution implemented by a public entity.

The security officer may issue orders regarding the compliance of agencies with guidelines or recommendations of the cybersecurity advisory committee; however, compliance with those guidelines or recommendations by non-executive agencies or county, municipal, or tribal governments shall be strictly voluntary.

The first meeting of the advisory committee shall be held no later than August 16, 2023, and meetings would be held every two months thereafter. The committee shall report to the legislative interim technology committees in November 2023. Before October 30, 2024 and on or before October 30 of subsequent years, the office shall update the reports, but presentations of reports shall be in executive session and are also exempt from IPRA.

The members of the cybersecurity advisory committee shall receive no pay for their services as members of the committee, but shall be allowed per diem and mileage pursuant to the provisions of the Per Diem and Mileage Act.

The bill also provides that, once effective, all functions, personnel, money, appropriations, records, furniture, equipment, supplies, and other property pertaining to cybersecurity or information security of the department of information technology are transferred to the cybersecurity office and that contractual obligations of the department of information technology for cybersecurity or information security services are binding on the cybersecurity office.

The bill notes all references in law to the chief information security officer of the department of information technology shall be deemed to be references to the state chief information security officer and that the chief information security officer for DoIT shall become the initial state chief information security officer.

The bill previously appropriated $300 thousand to the cybersecurity office in FY24 for staff and operations and for expenses of the cybersecurity advisory committee. However, HAFC amendments removed the appropriation.

The effective date of this bill is July 1, 2023.

FISCAL IMPLICATIONS

The bill no longer appropriates $300 thousand from the general fund to the cybersecurity office in FY24 for staff and operating expenses and for costs of running the cybersecurity advisory council under HAFC amendments. Therefore, fiscal impacts are limited to operating budget impacts.

The bill does not require DoIT to develop service rates for cybersecurity services provided by the department to other agencies or entities. However, any additional service rates to be created for cybersecurity services would have an impact on the general fund within agency operating budgets because they are expected to pay those rates. If cybersecurity services are not supported by rates paid by other entities as an enterprise service, the cybersecurity office will need to receive direct funding to support the provision of such services, which would have a similar budgetary impact on that office's general fund operating budget. The structure by which the office will support the provision of cybersecurity services is unknown and not provided for in this bill.

However, in terms of operating budget impacts for the office, DoIT cites a recent study by the National Association of State Chief Information Officers (NASCIO), reporting "the average spend on cyber efforts is around 10 percent of the annual IT operating budget including compliance. In addition, the previous study indicated the average business will invest between 6 percent and 14 percent of its annual IT budget in cybersecurity."

In FY22, DoIT finds total IT operating cost across state government entities is estimated at $280.6 million, but that is likely "understated since many state agencies do not have an IT operating budget per se because the IT function may be included in program support or could be operating elsewhere within the agency." Using the data mentioned, DoIT provides the below tables "to show what DoIT cybersecurity budget should be and the overall cybersecurity budget for the State executive. The estimated overall budget does not consider the judicial and legislative branch as well as school districts, other governmental entities including counties, municipalities, and tribal."

Estimated Cyber Budget - % of DoIT's IT Operating Cost of $77.7 million				
6%	8%	10%	14%	***Average***
$4,662.0	$6,216.0	$7,770.0	$10,878.0	***$7,382.0***

Estimated Cyber Budget - % of State IT Operating Cost of $280.6 million				
6%	8%	10%	14%	***Average***
$16,836.0	$22,448.0	$28,060.0	$39,284.0	***$26,657.0***

Therefore, DoIT expects the office will need an operating budget of around $8.8 million in FY24, of which an expected $5.2 million would be transferred from the DoIT operating budget, and $10 million in FY25 that would be needed from general fund revenues to support the office. As such, the total estimated operating budget impact for the office is $20 million recurring over three years, but resulting in an estimated net impact of $13 million after taking into consideration those funds to be transferred from DoIT in FY23 and FY24.

Further, the bill provides that all cybersecurity "functions, personnel, money, appropriations, records, furniture, equipment, supplies, and other property pertaining to cybersecurity or information security" be moved from DoIT to the office. DoIT's FY23 operating budget is $77.7 million, which DoIT notes includes close to $1.2 million for the cybersecurity functions within the Compliance and Project Management Program. That amount would be removed from the DoIT budget as a negative operating budget impact in FY23 and would in turn result in a positive budget impact on the office of an equal amount that year, resulting in no net change in total operating funds for this purpose in the first year. In its FY23 operating budget, DoIT has 5 FTE related to cybersecurity; the deputy chief information officer, two IT project manager positions, an IT security and compliance position, and an IT systems administrator. For that program, the average FTE cost is $138 thousand per FTE, so the above total budget amount to be transferred should include an estimated $414.5 thousand from the DoIT operating budget to the office for staff. Identifying the required items and functions to be transferred and undergoing such a transition will likely result in additional administrative needs, the costs of which are unknown.

The General Appropriation Act for FY24 also proposes an increase of $4 million in recurring funding for DoIT's cybersecurity services, so those funds would also be transferred from the department as a negative operating budget impact and would be transferred to the office in FY24, at which point all cybersecurity funding within the operating budget should be accounted for and transferred; therefore there is no expected fiscal impact on DoIT into FY25.

Public members of the new cybersecurity advisory council or subgroup established by SB280 may receive per-diem and mileage reimbursement in accordance with Sections 10-8-1 through 10-8-8 NMSA 1978 (the Per Diem and Mileage Act). Mileage costs would vary widely and are difficult to estimate. However, based on the rate of $155 per day for the 17 members, per diem would have a minimal fiscal impact, likely less than $20 thousand annually. Assuming one meeting every other month, the total estimated per diem costs to operate the council would be $15.8 thousand.

Senate Floor amendments to SB280 require the New Mexico Association of Counties and the Municipal League to appoint members of the advisory committee to represent counties and municipalities, respectively, which will likely require some administrative work to identify individuals with the needed knowledge of cybersecurity issues. It is unclear if the Municipal League or Association of Counties would incur costs to appoint these members, but members would not be compensated by those entities and would only be paid per diem as provided for in the act, so costs are likely minimal.

SIGNIFICANT ISSUES

DoIT provides the following:

> The State of New Mexico has of 75 agencies, and multiple boards and commissions. In addition, the state has 33 counties, 19 pueblos, 106 municipalities and 189 school districts. There are other critical infrastructure entities that provide services impacting the citizens of New Mexico. Currently, the state does not have a single pane of glass view into the state's cybersecurity preparedness, governance, and posture. A centralized function as the bill implies, where the Cybersecurity office with a State Chief Information Security Officer is responsible for leading cyber efforts will strengthen the overall posture of the State IT [eco]system.

The bill establishes the position of state chief information security officer (CISO) in statute, which is a best practice in establishing cybersecurity governance structures in state government. For instance, according to the National Conference of State Legislatures (NCSL), at least eight states—Arizona, Colorado, Florida, Kentucky, Massachusetts, Ohio, Utah, and Washington—statutorily require a statewide executive-branch CISO position or positions in state government. Other states have created CISO positions through executive orders or agency actions. Responsibilities of the CISO usually include creating statewide security policies and IT standards, requiring information security plans and annual assessments or reporting, and requiring periodic security awareness training for employees. CISOs with this type of government-wide authority are better equipped to coordinate and enforce these security measures. The SFC substitute for SB280 specifies this position is a classified position and is not an appointed position, which should provide some level of transparency and accountability in the hiring process to ensure the selection of a skilled applicant for the position.

Further, NCSL notes some states—including Georgia, North Dakota, Washington, and West Virginia—have recently passed legislation to require state agencies and, in some cases, local entities to report cyber incidents to a central office. SB280 may help achieve this, as it includes provisions requiring the cybersecurity office to be a resource to local governments, as an example.

However, as noted by NMAG, it is unclear what the expectation is of being a "resource" for local governments as provided in Section 3. It is also unclear how the department or office is expected to administer those resources and if there would be an additional cost. It is likely there would be additional administrative expectations for the office that do not currently exist at DoIT, so the office may need to establish new mechanisms for communicating and providing such resources to local governments. The office could likely benefit from coordination with other entities that have established communications and relationships with local governments such as the Local Government Division of the Department of Finance and Administration, the New Mexico Association of Counties, or Councils of Government.

Regarding data security laws, NCSL notes data security laws—which have only been enacted in recent years—requires governments or businesses take specific measures to protect sensitive information from unauthorized use, destruction, modification, or disclosure. As of 2018, NCSL notes that New Mexico has data security laws, but they only apply to businesses. At least 12 states have data security laws that apply to both business and government and at least 35 states enacted bills in 2021 to provide for strengthened data security measures to protect government resources.

However, the Department of Finance and Administration (DFA) notes:

> Data classifications and policies introduce the probability of data being incorrectly categorized and impacting the services provided by an agency, municipality or county. This in turn will impact how services are provided, revenue, and significant delays to business lines within an agency, municipality, or county. All three are listed as the bill does define adoption of initiative by public bodies.

In 2019, NSCL reported at least five states require public record exemptions for cybersecurity, which allows for exemption of cybersecurity information from disclosure. States with these laws require exemptions for records that contain network schematics, hardware and software configurations, and encryption, or the bills have provisions exempting public meetings that

would disclose such information. The SFC substitute for SB280 allows meetings and materials of the committee to be open to inspection unless determined the information would result in a vulnerability or exposure, which can help improve transparency while providing a needed layer of security over sensitive data. However, NMAG notes, because "the Cybersecurity Act also creates a new exemption to both the Open Meetings Act … both Acts may need to be amended to reflect the addition of a new exemption."

At least 18 states have a cybersecurity strategic plan in place, according to the National Association of State Chief Information Officers (NASCIO). The bill notes the advisory committee shall assist in the development of a state cybersecurity plan but does not provide descriptions or requirements for what should be included in that plan. According to federal guidance, a cybersecurity plan should include detailed, actionable plans for identifying, protecting, detecting, responding to and recovering from cyber incidents. The plan should include things like a spend plan, an asset inventory, and an overview of the state's detection or recovery processes to be implemented in the case of a cybersecurity incident.

The Department of Homeland Security and NASCIO believe cybersecurity should be governed as a strategic enterprise across state government. An interim working group of the Legislative Finance Committee met in 2022 to look at centralization as a potential policy strategy for governing and overseeing cybersecurity. This centralized approach is recommended by many experts, including NASCIO, and is provided for in the bill, requiring the office to develop a centralized cybersecurity data breach reporting process. Centralization is achieved by "essentially placing decision-making authority on cybersecurity in one or more central organizations and, in many cases, embedding cybersecurity governance within the state's centralized information technology services organization." However, there are many state agencies and independent entities that operate some form of cybersecurity program, and it is unclear if those functions or existing funding would be required to be moved to the office under the provisions of this bill, and many state entities will likely continue to maintain their existing FTE and other contracts related to cybersecurity within their operating budgets unless explicitly required to be moved to the office.

Nearly half of states—including New Mexico—do not have a separate state cybersecurity budget line item but instead include cybersecurity as part of the overall state IT budget. States that do have a cybersecurity budget line item established it through their state CISO (14 percent), statute or law (10 percent), executive order (10 percent), or administrative rule (6 percent). According to an analysis by DoIT, the state's total IT operating costs over the past four fiscal years totaled $957 million. If funded to a level similar to the private sector, an estimated 10 percent or an estimated $20 to $25 million per year would be needed for cybersecurity in New Mexico just for state agencies. It is unclear if the provision in SB280 requiring all cybersecurity-related functions and funding be moved from DoIT to the office will provide adequate funding for the establishment of such an office or to engage in the needed activities as provided for in the bill. However, the SFC substitute for SB280 includes a $300 thousand appropriation to assist the office with startup costs in the meantime until such resources can be transferred from DoIT to the office.

Although some of New Mexico's cybersecurity operations and policies are housed within DoIT, state cyber operations are siloed in different agencies, which is significantly more expensive and difficult to maintain compared to alternative structures. In 2018, only two states still operated a decentralized system while 15 states were operating a hybrid structure, which offers more

flexibility and economies of scale while allowing individual agencies to retain some level of purchasing power. To strengthen governance, many states have mandated or created cybersecurity advisory councils, which would be accomplished in New Mexico through this bill.

DFA notes in prior analyses that the bill may not consider "complex security issues related to each individual agency, municipality, or county. Each state agency for example may have unique security requirements, federal reporting requirements, and annual audit requirements. Standardization of protocols and policies is a solid step forward; however, falls completely short of addressing the needs of each individual agency." However, the bill only requires the office to set "minimum" security standards, so it is likely the intent of the bill is to allow agencies to maintain some level of flexibility and independence in implementing cybersecurity protocols and services.

In addition to establishing minimum security standards, NMAG, in prior analyses, notes the bill "provides the cybersecurity office with rulemaking authority. However, the Cybersecurity Act does not state whether the rulemaking authority is subject to the State Rules Act or if the rules adopted would be legally binding on other agencies."

However, DoIT previously provided the following analysis regarding rules:

> Section 3(B)(1) of the bill authorizes the cybersecurity office to adopt and implement rules establishing minimum cybersecurity standards and policies. This provision could be misconstrued to require adoption of rule to mandate cybersecurity practices. Under the State Rules Act, the minimum period of time required to promulgate a rule is approximately 90 days. In practice, most rule making proceedings extend beyond six months. Because of the rapidly evolving nature of cybersecurity threats and solutions, rules could not be promulgated in time to protect state information technology systems from emerging threats. Although rules should establish processes for issuing mandates, the processes should allow for extremely rapid action by the office. Under current language of Section (3)(B)(1), rapid implementation of cybersecurity solutions may not be possible.

Related to concerns regarding non-executive agencies, the NMAG noted in prior analyses:

> Section 5(G) provides authority of the security officer to issue "orders" that are defined as "strictly voluntary." The term "order" in administrative law is almost always a mandatory directive that compels someone or something to do something, or is a final decision that decides and issue and is binding. Orders or other forms of decisions in administrative law are generally subject to judicial review as a matter of right or as a discretionary review under Rules 1-074 or 1-075 NMRA. Calling what is an advisory letter an "order" in SB 280 may cause avoidable confusion regarding its purpose and effect and should use a different term.

PERFORMANCE IMPLICATIONS

DFA noted previously:

> DoIT is already doing scans and risk assessment reviews monthly, of which agencies are required to participate in, and scores, like CISO Scores, are currently reported at Cabinet level. Agency auditors are also required to include IT security compliance testing in their annual audit. As part of these audits, IT Departments are subject a separate strenuous audit which is separate and disclosed in the audited financial statements.

DoIT currently implements scanning and risk assessments for all executive branch agencies, and presumably under SB280 these services and contracts would need to be moved under the purview of the new office. It is unclear if this could be accomplished with a seamless transition of services or if there would be an interruption of that service in the transition to the office. Additionally, the department currently has several performance measures related to cybersecurity scanning and remediation which would no longer be relevant to DoIT under the provision of this act. Performance indicators would likely need to be revisited in the context of the General Appropriation Act to ensure measures are consistent with the intended requirements of the office and were not duplicative of other existing DoIT measures. DoIT previously noted:

> The pace of establishing a robust cybersecurity program for the State has been limited due to the federated model and insufficient recurring budget. It may require additional time for the state to meet its objectives as planning, standards and baseline needs to be established. Compliance activities must be completed across the State IT ecosystem for an effective, repeatable process and accurate reporting.

Further, DoIT notes the state's federated and fragmented model may result in delays in the implementation of the needed cybersecurity programming and establishment of the office, noting that "ramp up time could vary. Coordination with various federal oversight agencies and compliance requirements may introduce potential delays."

DFA previously noted the following:

> Probability of delays and misclassification of data will impact agency's ability to conduct business. Cybersecurity could become issue when establishing new lines of business under Governor's directive - case in point: creation of Emergency Rental Assistance Program. As part of its build and implementation all IRS1075 and PII standards were considered at the outset by internal teams.

DoIT also previously noted:

> Hiring much needed cyber security skillset across the state is an issue and potentially could impact the objectives. At present each entity defined in the bill has a need to hire resources by competing in the marketplace, increasing cost of doing business and not providing value for taxpayer dollars. Outdated and inadequate job classification and compensation mechanism and structure for IT and Cyber skill set can impact the effectiveness of the program for the state and other political subdivisions.

ADMINISTRATIVE IMPLICATIONS

DFA notes the possible duplication of annual audit processes and time involved with the audit, and notes the office will need clearly defined appeal processes to address misclassifications of data.

As noted, there may be additional needs for DoIT to identify the needed functions and funding to transfer to the office, but the extent of that need is not currently known. However, the agency provides; "SB280 provides the Cyber office the necessary authority and oversight to bring all executive agencies to a nationally established framework without impacting their independence or autonomy of their business objectives of other entities outside of the executive branch." Further, the appropriation provided for in the SFC substitute of SB280 should assist the office in

meeting its administrative needs while DoIT identifies the resources to be transitioned to the office.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

The bill relates to Senate Bill 269, which attempts to amend the DoIT Act.

The bill also relates to the General Appropriations Act of 2023, which includes $10 million to DoIT for cybersecurity, including $3 million to assist the Regulation and Licensing Department with remediation of a recent cyber-attack, $3 million to DoIT for cybersecurity for higher education, and $2.5 million to DoIT for cybersecurity at public schools and school districts. These funds would be transferred to the office, once established under this bill.

AMENDMENTS

DoIT previously proposed amending Section 3(B)(1) to read:

(1) Pursuant to the State Rules Act, adopt and implement rules to govern or implement any function delegated to the office in this Act, including rules to establish cybersecurity policies, to organize the office and its operations, to facilitate rapid deployment and implementation of cybersecurity standards and guidance and to manage cybersecurity incident reporting.

This amendment was not adopted in the SFC substitute for the bill or in Senate Floor amendments to the bill.

JH/ne/JH/rl/ne/JH/ne