November 17, 2020

MEMORANDUM

TO: John Arthur Smith, Chairman, Legislative Finance Committee
Patricia A. Lundstrom, Vice-Chairwoman, Legislative Finance Committee

FROM: Janelle Taylor Garcia, Ph.D., Program Evaluator, LFC

THRU: David Abbey, LFC Director
Jon Courtney, Ph.D., LFC Deputy Director

SUBJECT: Status of Cybersecurity

Summary – Since 2018, New Mexico state and local government, hospitals, public school districts, and higher education institutions have been victim at least 28 cybersecurity and ransomware attacks. This memo is an update on the status of cybersecurity projects within the Department of Information Technology (DoIT). Since 2018, the state has appropriated a total of $7 million to prevent cyber-attacks and manage the associated risks. However, most of those dollars have supported planning and pilot-type activities, and very few widespread protections for state government have been set into place. Moving ahead, LFC staff recommend DoIT develop a state cybersecurity plan that outlines the state's disaster management plan and cybersecurity posture.

Cyber-attacks threaten government operations and can be costly. With seven attacks in 2018 and 15 attacks in 2019, the number of cyberattacks in New Mexico has increased (Attachment 1). However, New Mexico does not have a number of protections in place deemed best practice by other states or national organizations including processes for reporting cyber incidents, and mandatory training for employees. For example, NM does not have a uniform cybersecurity process for reporting cyber incidents, or for entities seeking assistance. In recognizing they had a fragmented cybersecurity system, the Iowa Information Security Division began offering cybersecurity awareness training for county and city governments, schools and hospitals, and worked with the Secretary of State's Office to enhance cybersecurity resilience of election infrastructure. Additionally, cybersecurity awareness training is a best practice to help employees protect themselves and their employer against cyber-attacks and threats. This type of training empowers employees with up-to-date knowledge on how to recognize and mitigate a cyber-threat. New Mexico does not require state agency employees to participate in cybersecurity training, and the National Conference of State Legislatures (NCSL) reports that while every state offers cybersecurity training for state employees, it is only mandatory for employees in 16 states. Texas and Oregon require annual cybersecurity training to occur on an agency-by-agency basis, and all state agencies must submit a cybersecurity plan annually.

DoIT reports that in February 2020, they notified IT leads and state agency Chief Information Officers (CIO) of the department's cybersecurity awareness training initiatives available to state agencies beginning in March. DoIT issued a purchase order to Inspired Learning to deploy online training for up to 7,200 state employees. However, due to COVID-19 DoIT postponed the training. DoIT employees completed mandatory cybersecurity awareness training, followed by a pilot rollout in late November. DoIT anticipates

deploying online cybersecurity awareness training to state agencies in December 2020. Although cybersecurity awareness training is not mandatory statewide, individual agencies, such as, Taxation and Revenue, and the Department of Health and Human Services require annual IT security training for their employees.

The Department of Homeland Security (DHS) and the National Association of State Chief Information Officers (NASCIO) believe that cybersecurity should be governed as a strategic enterprise across state government and other public sectors in six areas; workforce and education, strategy and planning, budget and acquisition, risk identification and mitigation, incident response, and information sharing.

Source: NASCIO, 2017

With an increased number of employees working remotely, and schools transitioning to online teaching and learning due to the coronavirus pandemic, NASCIO predicts the number of ransomware and hacking incidents will increase in 2020 and beyond. A National Council of State Legislatures (NCSL) survey of top IT security officers in all 50 states identified the top three issues affecting states' cybersecurity: budget, talent, and increasing cyber threats. While any individual, government, or business is a potential victim, school systems are particularly vulnerable because they hold troves of private data, and school districts often lack the resources to fend off intruders. With funds appropriated through the General Appropriation Act of 2020 (Section 5), the New Mexico Public Education Department will be completing cyber security and data system upgrades.

In April 2020, DoIT hired a Chief Information Security Officer (CISO). Prior to April, DoIT was operating with the expertise and guidance of a contracted CISO. Since hiring the CISO, DoIT has begun to develop and implement a few best practice initiatives, such as the organization of an Enterprise Cybersecurity Upgrade (ECU) advisory committee. In addition, DoIT reports they have the basic framework of a disaster management plan that was developed around 2010, but there has been no follow up or updates to the existing plan. Additionally, NMAC 1.12 is not up to date to reflect the latest developments and security practices in informational technology including adequate segregation of security and IT operations. According to DoIT, until revised policies are vetted and approved, the DoIT 2010 IT Security Policy is still in effect and are under review by Deloitte, as specified in contract deliverables. It is a recommended best practice, in addition to developing a business continuity and disaster recovery plan, DoIT should develop a state cybersecurity strategic plan. Illinois and Texas are examples of two states that have state cybersecurity strategic plans, which allow for an efficient and collaborative culture, place high value on protecting state data and information, and create a protected and resilient cybersecurity

environment. While DoIT has recently secured a CISO, a more formalized governance structure should be delineated, as one person cannot handle all of the intricacies involved with state cybersecurity.

In September 2020, DoIT received approval to hire an IT Project Manager and an IT Security and Compliance Administrator who will directly support the CISO in developing a comprehensive cybersecurity program. The two additional positions will ease the CISO's workload in supporting the Office of Cybersecurity within DoIT, and the governance structure is being evaluated by Deloitte as one of the deliverables for the development of a Cybersecurity Control Framework.

Since FY2018, the legislature has appropriated a total of $7 million dollars to support cybersecurity efforts, but funding has not accomplished intended goals. These appropriations were to perform a statewide cybersecurity assessment to identify and implement security tools for compliance monitoring and risk management. Also, to plan, design, construct, and implement a statewide enterprise cybersecurity operation center system.

Table 1. Department of Information Technology
Cybersecurity Appropriations and Revenue

Fiscal Year	Funding Source	GF Amount	Total	Purpose	Amount Expended/Encumbered	Amount Reverted
FY19	Laws 2018, Chapter 73, Section 7(11)	$1,000,000	$1,000,000	Perform a statewide cybersecurity assessment and identify and implement security-related tools for compliance monitoring and cybersecurity risk management.	$951,104	$48,896
FY20	Laws 2019, Chapter 277 , Section 32(5)	$6,000,000	$6,000,000	Plan, design, construct, and implement an enterprise cybersecurity operation center system, including the purchase and installation of equipment, for state agencies statewide.	$2,951,822	N/A
Total		$7,000,000	$7,000,000		$3,902,926	

Source: LFC Files, 2020

A $1 million appropriation for a statewide cybersecurity assessment has not yet resulted in a completed assessment

In 2018, the Legislature appropriated a $1 million to DoIT to perform a statewide cybersecurity assessment, to identify and implement security-related tools for compliance monitoring and cybersecurity risk management. With the appropriation and project certification, DoIT initiated its ECU project in November 2018, with $80 thousand in certified funds. The project charter states the venture will be a multi-faceted undertaking, including:

- strengthening the state's security workforce by retaining new talent and growing the pipeline;
- creating a robust CISO by leveraging multiple vendor contracts;
- creating an enterprise library of security policies; maturing incident response abilities in partnership with vendors and state agencies, and;
- utilizing enterprise solutions across the state, with strong executive support for all-agency participation.

According to the project's charter, cybersecurity incidents are currently identified and remediated on a case-by-case basis, at the individual agency level. DoIT and other agencies have mostly siloed hardware and equipment, although there appears to be an interest in cooperation and collaboration, as the complex landscape requires in order to be effective.

The project was to occur in the following phases with identified product deliverables.

Table 2. Department of Information Technology
Enterprise Security Upgrade Project Phases

Phase	Work to Be Performed	Product Deliverables
I	Initiation and planning	charter project management plan risk assessment contract requirements CISO plan
II	Planning for foundational cybersecurity framework for the enterprise	current state assessment stakeholder/partner approach define governance structure outline policy library
III	Implementation for initial enterprise concept of operations; policy library; operationalize governance structure & partnership plan	enterprise cybersecurity governance policies and procedures library security operations center threat/monitoring tools
IV	Standardization and stabilization	fully operationalized cybersecurity enterprise framework

Source: ECU Project Charter, 2018

If DoIT had a state cybersecurity strategic plan in place, as is best practice, formal mechanisms and framework would already exist, which would allow the state to address the changing cybersecurity landscape, and would enable collaboration across state agencies.

According to DoIT, with part of the $1 million appropriation, they engaged RiskSense Inc., with its product suite, and identified and implemented security related tools for compliance monitoring and cybersecurity risk management.

DoIT certified a change request for the ECU project for $619 thousand in April 2019 to conduct a statewide risk assessment but instead, contracted with RiskSense, Inc. for a quarterly vulnerability scan pilot project. In June 2019, DoIT announced a pilot project to provide quarterly vulnerability scans to state agencies' CIO's to provide a tool to assist IT staff to prioritize security risks, assign remediation tasks, and measure progress. At a cost of $593.9 thousand, DoIT contracted with RiskSense, an IT security expert that supports several state organizations, to perform quarterly vulnerability scans. Through the pilot, RiskSense performed vulnerability scans on state assets for 42 executive agencies and three non-executive agencies (as of August 2020). The resulting data is loaded into the RiskSense platform – a tool to support analysis and remediation – and shared with DoIT. Although DoIT plans to use the information for cybersecurity-related trend analysis, it is not clear how DoIT communicates the results to participating state agencies, and what type of remediation activities are underway. RiskSense cybersecurity vulnerability scans occurred during the fourth quarter of FY20, and DoIT reported that as of November 2020, RiskSense on boarded 43 of 67 agencies (64.2 percent). The vulnerability scans have a scoring system, and utilize a color-coded indicator of red, yellow and green, with green indicating less vulnerability and red indicating highly vulnerable. The score represents the organization's cybersecurity posture, measuring risk posed by vulnerabilities and identifies potential threats (Attachment 2). According to DoIT, the RiskSense, Inc. tool and portal for reporting is consistently tuned, and the effectiveness of the reports have improved within one year of the pilot rollout.

In December 2019, DoIT disseminated a 14-page survey to state agencies to identify the status of each agency's security posture. Although DoIT received 19 responses (38 percent response rate), DoIT has not compiled the results nor is it clear if DoIT conducted outreach to agencies that did not participate in the survey. The results of the security survey were to be used to capture individual

agency strategic plans and to assist in the creation of an overall state plan. To date, this has not been completed and it is unclear if there has been follow up with state agencies. If there were a plan in place to obtain the un-submitted surveys, this would aid DoIT in the development of a formal state cybersecurity strategic plan. DoIt reported that while the survey was intended to obtain the current security environment across state agencies, shifting priorities limited additional outreach to improve survey participation. DoIT requested state agencies to provide contact information for IT security leads to disseminate security guidance and advisories. As part of the FY22 IT Strategic Planning, DoIT requested state agencies to include some relevant security items in their plans.

DoIT did not request an extension for the $1 million appropriation expiring at the end of FY20, and reverted approximately $49 thousand to the general fund. This reversion of funds should not have occurred had a project manager been responsible for the oversight of the ECU project. Due to not hiring a project manager to oversee the project activities, there was no one held accountable for ensuring on-time delivery of project deliverables and work products, and to ensure the project plan was implemented appropriately.

DoIT spent $950 thousand on cybersecurity without a plan or project manager. As part of the ECU scope of work, a project manager was to be hired to lead project planning and manage the day-to-day operation. Additionally, the project manager was to provide; management-related and technical work as needed to ensure on-time delivery, lead the project team, plan and facilitate meetings, develop specified deliverables and work products, and ensure that issues and action items and risks were identified and addressed in a timely manner. DoIT continued the project without a project management plan. The previous DoIT Secretary reported the project management plan was in the process of being drafted, however, as of the date of this memorandum; DoIT has not provided neither the draft nor the final project management plan for the ECU initiative. DoIT reported that although they awarded ATA Services a contract for the ECU project manager in March 2019, and they contracted with Advanced Network Management (ANM) to provide IT security services including project management activities; due to changing priorities, ATA did not finalize the project management plan.

Prior to the hiring the CISO, the department contracted with Advanced Network Management (ANM) to provide IT security services for $251 thousand per year.
The ANM contract stipulated they were to provide expert cybersecurity support to plan, implement, and monitor improvements to DoIT's cybersecurity posture. The dates the contract was in effect were from February 2019 through February of 2020. According to the contract, ANM was to provide project management and technical implementation services for cybersecurity projects and participate as a virtual CISO for the agency. The contract further stipulated that ANM was to complete the following:

- Provide vulnerability management within the 12 months of the contract.
- Review weekly firewall reports and provide recommendations, as well as future planning
- Submit a status report, at least monthly, documenting work performed and upcoming tasks
- Work as the agency vCISO up to 20 hours per week, on site or remotely.
- Plan, lead and/or participate in security related meetings with agency staff
- Submit a monthly status report to the agency along with the monthly invoice.

In 2019 DoIT received $6 million in general fund capital outlay to plan, design, construct and implement an enterprise cybersecurity operation center system for state agencies statewide, however to date, has only expended $1.3 million dollars

Table 3. Department of Information Technology
Enterprise Security Upgrade Project Budget & Expenditures

	2019	2020	2021	Grand Total
Budget	$6,000,000	0	0	$6,000,000
Expense	0	$238,352	$986,943	$1,225,296
Encumbrance	0	$1,209,566	$516,960	$1,726,526
Pre-Encumbrance	0	$218,447	($218,447)	0
Available Budget	$6,000,000	($1,666,366)	($1,285,456)	$3,048,179

Source: LFC Files

The $6 million appropriation is authorized in FY19 through FY23, and due to the complexities and expertise needed to implement an enterprise operations center, the current DoIT secretary recognizes the critical need to establish a Cybersecurity Control Framework and as a result, DoIT awarded Deloitte a contract to develop a roadmap and framework. DoIT reports they are on track to expend appropriated funds as new project initiatives move forward, and are in the process of aligning the project funding, scope and phases at the next Project Certification Committee meeting.

As a state data center service provider, DoIT provides a secure facility and infrastructure to host various systems and/or applications used to support DoIT and other state agencies. Through a consolidated data center, DoIT is able to optimize the use of electrical power and mechanical systems and space allocation in a secure and environmentally controlled facility. Currently, state agencies have the option of utilizing the DoIT facility to host their applications or they can choose to only lease rack space to co-locate their own network systems within the data center.

Of 67 state agencies, DoIT is currently only hosting seven state agency applications, and 27 additional agencies are leasing space in the facility for their own equipment (Attachment 4). As per the project description of the cybersecurity operations center, the $6 million appropriation is to plan, design, construct, and implement an enterprise cybersecurity operation center system for state agencies statewide. However, with DoIT currently only hosting seven state agency applications, DoIT must increase this number to ensure state agencies are following cybersecurity best practices. The project plan states the $6 million will be used to purchase and install new equipment, however, is there a need for additional equipment if DoIT is only hosting applications for seven of 67 state agencies and leasing space for 27. State agencies should consult and evaluate DoIT's service offerings prior to expending state resources outside of the state on things such as cloud storage, and other hosting scenarios. This increases state agency cyber vulnerability. According to DoIT, state agencies are authorized to make decisions to maintain and operate their servers and associated applications independently.

In June 2020, DoIT awarded a $921 thousand contract to Deloitte for expert technical and management support for the ECU project. According to the contract, the project manager for this project will be the DoIT CISO. The contract further stipulates that Deloitte will plan, lead and manage the ECU project and shall perform technical work in collaboration with DoIT. The contract outlines project deliverables, which include the development of a project development plan (within ten days of project start), monthly project status reports (within thirty days of agreement execution), a cybersecurity risk assessment and policy review, and findings and recommendations to be shared with the agency (within 60 days of date

of agreement execution). Project findings and recommendations are to be provided to DoIT at 90, 120, and 150 days of agreement execution. As of November 2020, DoIT reported that Deloitte has delivered a set of comprehensive IT Security policies, a project management plan, Cybersecurity Control Framework, Communication Plan, a draft governance structure and draft Tools framework. DoIT will include several elements of Deloitte's project management plan as part of its project certification documentation to be presented to the Project Certification Committee in late November.

At least 26 states have created a formal, statewide cybersecurity task force, commission or advisory council or group in the past several years, as is a best practice as per the National Council on State Legislatures (NCSL). Successful IT governance is most effectively accomplished through the establishment of a formal governance committee made up of leaders of key agencies working with IT leadership to establish and monitor operations and investments. Of the 26 states with formal statewide cybersecurity advisory groups, most were created by executive order, and at least eight states created these initiatives through formal legislation. In addition, Georgia authorized legislative study committees in 2016 and 2017 to examine cybersecurity issues, as did Indiana in 2016. The State of Kansas has initiated several statewide initiatives aimed at improving the state's information security posture. A 2011 Executive Order centralized Kansas' information technology (IT). Prior to that, every state agency took care of their own IT issues, much like New Mexico. In addition, the Executive Order required all IT directors at agencies within the executive branch, to report to one central person, the Chief State Information Technology Officer. The Kansas Cybersecurity Act, signed in 2018, included a few key pieces related to IT security. The Act created a standalone agency, the Office of Information Technology Services (OITS). The Act permitted OITS to charge fees and provide guidance to other state agencies, and underscored the chief executives at the various agencies to remain responsible for their agency's IT security. For example, the chief agency executives are responsible to ensure that their agency has an IT security program, and each agency chief participates in an executive security training with the chief information technology officer. One caveat of the Act is that some agencies were exempt from the Act, elected offices (like the Attorney General) the agency that manages state retirement funds, and state universities. DoIT reported that Deloitte has developed a draft governance structure as part of its contract deliverables.

DoIT began an ECU advisory committee, but only began meeting in May of 2020. Committee members include, four DoIT employees (the Secretary, CISO, Deputy CIO, and the Director of Enterprise Services and Communications) and 11 other individuals from across state agencies, including at least two agency CIO's. While meeting agendas for the May and July meetings were not provided, the August meeting included updates from RiskSense, including new reporting features and updates to the RiskSense platform. Deloitte also presented their cybersecurity plan, project roadmap, and updates to the project. While DoIT has begun having advisory committee meetings, they need to establish a more formalized governance structure, and include all state agency stakeholders. DoIT reported that as part of Deloitte's contract, they have developed and suggested a tiered approach with steering, advisory, and working groups based on various state best practices.

Recommendations – Prior to appropriating additional funding to the Enterprise Cybersecurity Upgrade Project, the Legislature should consider requiring the Department of Information Technology to provide the LFC a detailed cybersecurity strategic plan. Such a plan should foster state and agency leadership engagement for cybersecurity initiatives, provide a proactive cybersecurity defense through insight and technology, ensure adequate knowledge of the workforce, and minimize the detection and response time for security events, and propose a sustainable revenue source for continued cybersecurity. Additionally, the strategic plan should establish cybersecurity outreach to increase awareness of cybersecurity best practices within all state agencies.

The Department of Information Technology should:

- Develop a business continuity plan and take the lead with state agencies in the development of their own business continuity plans.
- Hire a Project Manager for the Enterprise Cybersecurity Upgrade (ECU) Project. Although the DoIT Chief Information Security Officer is designated as the Project Manager in the Deloitte contract, a separate individual whose primary role is only the ECU should be hired to oversee the day-to-day operations and management of the project, as this is considered best practice.
- Establish a governance structure that allows key stakeholders to take part in the decision-making process and for determining priorities as they pertain to state cybersecurity.
- Develop a timeline to ensure all state agencies participate in quarterly vulnerability scans, DoIT must then develop a plan to communicate the results of the scans to participating agencies, and outline a remediation plan for agencies to follow.
- Develop a state cybersecurity strategic plan. Indiana and Texas are examples of two states that have state cybersecurity strategic plans that allow for an efficient and collaborative culture, place high value on protecting state data and information, and create a protected and resilient cybersecurity environment.

The Legislature should also consider**:**

- Developing legislation for the creation of a state cybersecurity task force to include state agency CIOs. This would allow DoIT to provide guidance and coordinated messaging to other state agencies, including mandatory cybersecurity training for all state employees.
- Developing legislation related to disaster management and cybersecurity. Current legislation does not mandate agency participation, and is open to wide interpretation.

Attachment 1.
Cybersecurity Incidents in New Mexico since 2017

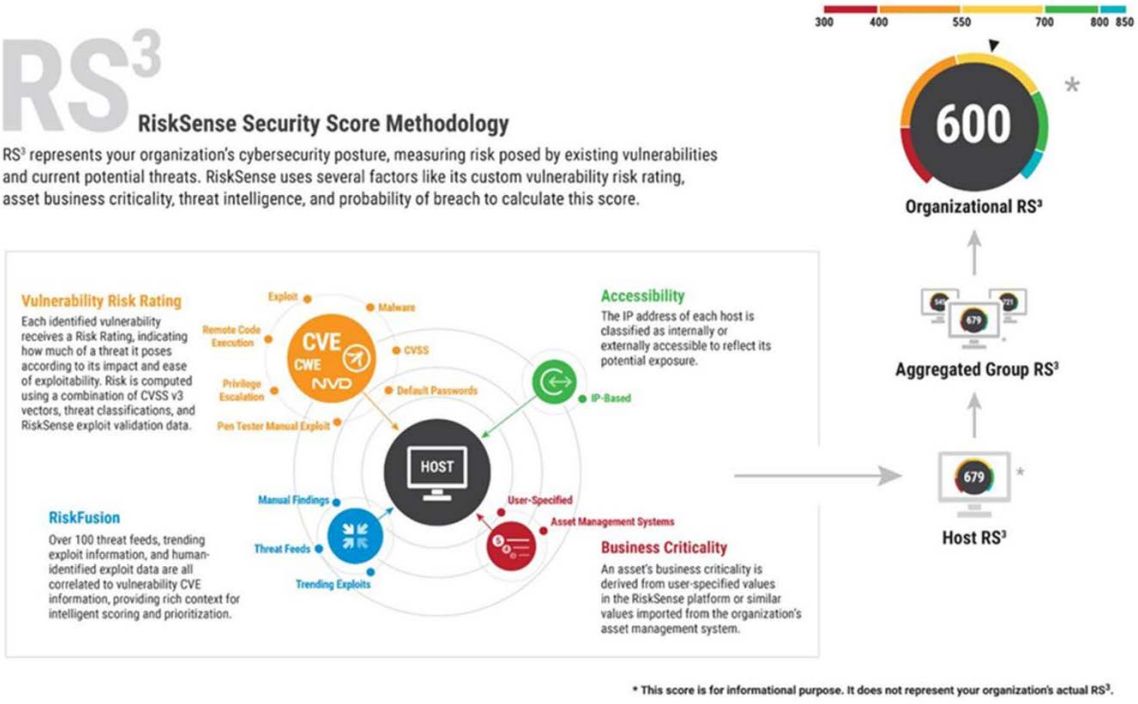
Year	Department/Agency	Cyber Issue	Cost
4/17/2017	University of New Mexico, Bernalillo County	2300 potentially exposed after server breached by hackers. UNM notified potentially affected individuals. Database accessed contained HR & financial information. University offered no cost credit monitoring to affected individuals.	Unknown
1/1/2018	City of Farmington Police Department, San Juan County	City of Farmington target of malicious activity, Virus infiltrates computers, Police Dept. offline as well as all other city departments.	$200,000 in recovery
7/13/2018	City of Alamogordo, Otero County	Phishing scam. Fraudulent emails probed employees into changing bank account information. Payments went through to faulty accounts. City has cyber insurance & police investigating.	Unknown
9/1/2018	NM Public Education Department, Santa Fe County	Phishing and spoofed email requests for payroll changes from the PED.	Unknown
9/1/2018	Santa Fe Public Schools, Santa Fe County	NM Office of the State Auditor received reports of potential criminal violations & suspected fraud associated with phishing & spoofed email requests for payroll changes.	Unknown
9/1/2018	Christine Duncan Charter School, Bernalillo County	Phishing scam. Fraudulent emails appearing to come from the Principal attempting to 'phish' financial account information.	N/A
12/18/2018	Lea County Government	Phishing scam. Fraudulent vendor sought payment of $32,500, employee paid the wire transfer. Officials learned of scam and reported to Lovington Police.	$32,500
1/29/2019	Las Cruces Public Schools, Dona Ana County	School system forced to disable network to stop spread of cyberattack. IT officials discovered infected servers & promptly removed them from network. Over 1,000 school are believed to have been attacked in total.	$300,000
7/1/2019	Gadsden Independent School District, Dona Ana County	Dozens of seniors did not after district officials discovered students hacked into district system and changed grades from February through April. 456 grades from various levels had been altered. Of the 55 students found responsible, 29 were seniors, and 26 were in 10th or 11th grade. Five were suspended & the others have various options to rectify their work.	Unknown
Jul-19	Gadsden Independent School District, Dona Ana County	Ransomware attack, prompted staff to shut down the internet and phone service. The effect of ransomware, RUYK	$1.9 million in restoration

8/2/2019	Presbyterian Healthcare Services, Bernalillo County	Personal information accessed following phishing cyberattack. Officials notified approximately 183,000 patients that their information was breached. Name, date of birth, Social Security among leaked information.	Unknown
9/20/2019	Rio Rancho Public Schools, Sandoval County	DDOS attack (denial of service). Overloading of network with large amount of data to make system crash and shut down all online sites.	Unknown
9/1/2019	Las Cruces Public Schools, Dona Ana County	LCPS confirmed it accidentally sent out an email containing social security numbers of vendors. Vendors advised to place fraud alert on their credit files as a precaution, and to check credit reports and financial history for signs of identity theft.	Unknown
10/10/2019	New Mexico Highlands University, San Miguel County	Ransomware cyberattack affected servers, some information was compromised. Midterms postponed by a week. Main website affected, created error messages when browsing. Classes cancelled for over one week.	$150,000
11/14/2019	Roosevelt General Hospital, Roosevelt County	Personal information system breached in malware cyberattack. IT department was able to secure & restore affected server. Names, addresses, DOB, SSN's, driver's license numbers, phone numbers, insurance & medical information, & genders of patients leaked.	Unknown
1/15/2020	NM Public Regulation Commission, Santa Fe County	Public utility regulatory agency hit in cyberattack. State Attorney General's office requested money for cybercrime unit. Additional state agency's website went down during attack.	Unknown
2/6/2020	San Miguel County	Unknown bad actors utilized ransomware during cyberattack, officials were unsure about extent of potential damage, personal or private information may have been leaked.	$250,000
2/7/2020	Bernalillo County	Phishing cyberattack, officials discovered bad actor's created fake business accounts that were subsequently paid, county IT assisted by FBI and other authorities.	$500,000
2/28/2020	Taos Municipal Schools, Taos County	Hackers demanded $5000 in cash ransom for return of the control to their digital services. Emails, class instruction & the district website were disabled as part of the attack. No money paid. District working with FBI to find responsible party.	Unknown
5/27/2020	Rio Arriba County	Officials stated that almost every server on network affected, backup servers were also affected by cyberattack, insurance company and federal law enforcement were notified.	Unknown

Jun-20	NMSU Foundation, Dona Ana County	Unusual network activity noticed. University moved quickly to contain any possible data loss and removed affected devices from network. After investigation, no evidence of theft or misuse of personal data.	Unknown
Jul-20	UNM Law School, Bernalillo County	Ransomware attack prevented students and faculty from accessing emails and shared files.	Unknown
	Clovis Municipal Schools, Curry County	One of several public entities in NM targeted in a payroll phishing scam, scammers did not get any money.	Unknown
	Albuquerque Public Schools, Bernalillo County	Volcano Vista High School network knocked offline by a malicious actor. School administration believed it to be a student or students.	Unknown

Source: LFC Files (2020)

Attachment 2.
RiskSense Security Score Methodology



Source: RiskSense, Inc. (2020)

Attachment 3.
Enterprise Cybersecurity Upgrade (ECU)
Project Expenditures

Vendor Name	Purchase Order Amount	Contract Amount	Contract Term Date	Contract or Purchase Order Description
Century Link	$87,016		9/15/2026	RiskSense Software Platform:Security software, cyber risk identifying application & database level risk
ANM Advanced Network Management Inc.	$162,65	$162,656	6/30/2021	Support maintenance and operation of the network, and cybersecurity for assets
ANM Advanced Network Management Inc.	$58,800	$58,800	6/30/2020	Professional Services to obtain expert and technical administrative
Technology Integration Group	$170,229	$170,229	11/17/2021	State email Software Support: Network Firewall Maintenance/support
Convergeone	$341,589	$341,589	11/17/2021	IT Hardware Maintenance: SmartNet Equipment Maintenance Renewal-Network Security
ANM Advanced Network Management Inc.	$4,961	$4,961	11/17/2021	Emergency Security Incident Response for Security Issues Statewide for all Agencies Tax Included
ANM Advanced Network Management Inc.	$66,740	$66,740	11/17/2021	Software Renewal/support: Splunk Enterprise-Standard Support Renewal (Existing License)Size=200 Gigabytes per day (07/01/19-06/30/2020)
ATA Services Inc.	$8,337	$253,000	12/31/2019	Expert management support for the Digital Government Initiative, Enterprise Cybersecurity Upgrade and for the Project Management Center of Excellence.

RiskSense, Inc.	$539,909	$593,846	6/30/2021	Contractor shall extend Task Item 3 in Deliverable Number 1 Attack Surface Validation for Networks
ANM Advanced Network Management Inc.	$100,000	$350,859	6/30/2020	Professional Services: To extend contract term, increase total hours for cybersecurity
ANM Advanced Network Management Inc.	$56,982	$200,000	6/30/2020	Network Security: Professional Services
Level 3 Financing Inc.	$308,637	$308,637	9/15/2026	RiskSense Software Platform Security Software, cyber risk application & database level risk
Carahsoft Technology Corporation	$53,669	$53,669	9/16/2026	RiskSense Security Rating Services-1st Party RiskSense SAS, 2 Month Subscription-Start Date 03/31/2020 FY20
Level 3 Financing Inc.	$95,162	$95,162	9/15/2026	RiskSense Software Platform to include tax, April 10-June 30, 2020.
TOTAL		**$2,747,165**		

Source: DoIT, 2020

Attachment 4.
DoIT Facility State Agency Hosting and Co-locating

Service | Agency	**Total Count**
Application Hosting	**7**
Department of Environment	
Department of Finance and Administration	
Department of Information Technology	
Department of Military Affairs	
Office of the Governor	
Personnel Board	
Public Education Department	
Co-Location	**27**
Aging and Long-Term Services Department	
Children, Youth and Families Department	
City of Santa Fe	
Corrections Department	
Cultural affairs Department	
Department of Environment	
Department of Finance and Administration	
Department of Game and Fish	
Department of Health	
Department of Information Technology	
Division of Vocational Rehabilitation	
Economic Development Department	
Educational Retirement Board	
Gaming Control Board	
General Services Department	
Human Services Department	
New Mexico Department of Workforce Solutions	
New Mexico Livestock Board	
NM Interactive, LLC	
Office Of Superintendent Of Insurance	
Public Education Department	
Public Regulation Commission	
Regulation & Licensing Department	
Santa Fe County	
Secretary of State	
State Engineers Office	
Taxation and Revenue Department	
Co-Location & Application Hosting (Both Services)	**4**
Department of Environment	

Department of Finance and Administration	
Department of Information Technology	
Public Education Department	
Web Hosting	**12**
Administrative Office of the District Attorney	
Board of Examiners for Architects	
Board of Nursing	
Department of Environment	
Department of Finance and Administration	
Department of Information Technology	
Human Services Department	
New Mexico Board of Medical Examiners	
Public Education Department	
Public Employees Labor Relations Board	
Public Employees Retirement Association	
State Engineers Office	

Source: DoIT, 2020