County Counsel
Christopher L. Beck

Assistant County Counsel
Emily Fox

Deputy County Counsel
Jeff Hughes
Janet Carson

OFFICE OF THE
COUNTY COUNSEL
Mono County

South County Offices
P.O. BOX 2415
MAMMOTH LAKES, CALIFORNIA 93546

Telephone
760-924-1700

Risk Manager
Jay Sloane

Paralegal
Kevin Moss

June 10, 2025

Mono County Grand Jury
Honorable Judge Mark Magit
Presiding Judge of the Superior Court
100 Thompsons Way
P.O. Box 1037
Mammoth Lakes, California 93546

RE: Response to the Mono County 2024-2025 Grand Jury Report regarding Mono County Cybersecurity Preparedness

To the Honorable Judge Magit Grand Jury Members:

Please consider this letter and Attachment A as the Board of Supervisors' responses to the 2024-2024 Grand Jury Investigation Report entitled Mono County Cybersecurity Preparedness in accordance with Penal Code Sections 933 and 933.05.

Mono County thanks the Grand Jury for its attention to these critical issues and we appreciate the concerns raised in this Report. Our Board looks forward to continuing to encourage and direct our IT Department to pursue solutions and systems that will improve the cybersecurity of Mono County.

Thanks and Best,

Emily Fox
Assistant County Counsel

Cc:
Nancy Licari, Staff Secretary to the Grand Jury

Enclosures:
Attachment A, "Board of Supervisors Responses to the 2024-2025 Grand Jury Report Entitled Mono County Cybersecurity Preparedness"

Responses to Investigation Report: Mono County Cybersecurity Preparedness

Findings:

F2: The Payment Card Industry (PCI) self-assessment questionnaire (SAQ) process inadequately involves IT resulting in a lack of IT awareness of the PCI Compliance process and errors on attestation reporting.

Response to F2:

The Board agrees in part and disagrees in part with this finding. Mono County IT itself does not store or process customer credit cards, and as a result has not been involved in PCI. Departments that receive credit card payments do so via 3rd party vendors. As such, payment systems decisions are determined by Finance, managed by the departments that use them, and should go through a contract, technical, and security review process by IT. Nonetheless, Mono County IT can be equipped to better assist departments in managing their obligations with respect to PCI.

Implementation of F2:

The Board will direct IT will train staff to be aware of PCI and SAQ requirements in order to better assist other county departments beyond the existing technical and security review of all vendor contracts that involve software or some other nexus with IT. IT will work with Finance to identify the correct SAQ form to be used during the self-assessment process and will partner with Finance and other departments responsible for processing customer credit cards to complete the SAQ and will provide input where appropriate.

While the Board recognizes that IT cannot control certain customer actions that may jeopardize data, such as when customers send credit card information over plain text email messages, the Board will encourage IT will optimize the Office365 environment and implement data loss prevention policies according to best practice to secure data from the point of receipt forward, such as ensuring that any reply to a plain text email with sensitive data will be encrypted.

Implementation Timeline for F2*:*

The Board will direct IT to implement these solutions by close of Fiscal Year 25-26.

F3: The lack of immutable backups results in increased risk of disruption to important County operations due to a ransomware attack.

Response to F3:

The Board agrees with this finding. The Board recognizes and takes seriously the importance of reliable accessible backups. The Board acknowledges that there are always ways to improve the backup technology that we use beyond what is required.

Implementation of F3:

The Board will direct IT to research available and practical immutable backups and the possible implementation strategies for Mono County's needs. In doing so, IT will seek input from and collaboration with departments to identify their most critical systems that require

immutable backups. IT will also work to develop a procedure for the implementation of immutable backups that then meets departmental needs.

As the implementation of immutable backups will require additional, currently unallocated resources, the Board will direct IT will create a plan for immutable backups that includes those resources in a future budget process for the Board to review.

Implementation Timeline for F3*:*

As immutable backups implementation requires currently unallocated resources, the Board expects that IT will include adequate resources in the Fiscal Year 25-26 budget process and implement within that timeframe. Due to the sensitive nature of these discussions, the Board of Supervisors expects to be notified in closed session of significant cybersecurity risks pursuant to newly enacted legislation permitting cybersecurity risks to be discussed in that forum.

F4: Computing devices, no longer supported by the vendor, are present in the environment resulting in an increased risk of cybersecurity vulnerabilities and attacks.

Response to F4:

The Board agrees with this finding. IT acknowledges that there are pieces of equipment that are past their End-Of-Life (EOL) still operating in our environment. Currently we operate under a Technology Refresh/Internal Service Fund (ISF) that was established in 2014. The ISF was meant to ensure that equipment, including desktop devices, servers, and storage) could be replaced in an efficient fashion as that equipment reached its EOL. The ISF was designed to guarantee adequate funding for those replacements. Each department contributes to the fund annually in accordance with the number of employee positions they have and the number of devices they have in service. However, ISF funding has not always been adequate to replace all the equipment. Relatedly, IT has struggled to maintain adequate personnel resources to replace all equipment.

Implementation of F4:

New equipment has already been purchased to replace identified network equipment that is at EOL. IT has developed a schedule for the removal of the obsolete equipment and the installation of the new equipment.

Replacement equipment that is designed to replace equipment at its end-of-sale is scheduled for purchase in Fiscal Year 25-26. IT will develop a similar schedule for the removal of the obsolete equipment and installation of the new equipment.

As budget has not always been adequate to replace all EOL and end-of-sale equipment, IT will update its procedures and monitor the costs of replacement equipment to make the ISF more effective going forward.

The Board will review any additional personnel resources, such as another Network Specialist position, during future budget processes and allocation adjustments in order to ensure IT is able to meet schedules for removal and installation of equipment.

Implementation Timeline for F4*:*

Replacement of equipment designed for end-of-sale is scheduled for purchase during Fiscal Year 25-26. IT will include additional resources in the Fiscal Year 26-27 budget process as needs are identified.

F5: The lack of consistent periodic external penetration testing and vulnerability scans results in unknown potential exploits which increases the risk of cybersecurity incidents.

Response to F5:

The Board agrees with this finding. IT recognizes and takes seriously the importance of identifying and understanding potential points of vulnerability to cyberattack. The environment is currently monitored by a 24/7 Security Operations Center and activity is monitored by IT staff. Potential risks are researched and IT staff take the necessary steps to mitigate those risks. Additional security exercises and testing are beneficial ways of protecting the environment.

Implementation of F5:

The Board will encourage IT will explore additional penetration testing strategies and vendor relationships. To date, IT has pursued low or no-cost services from state and federal partners for penetration testing.

Implementation Timeline for F5*:*

As penetration testing requires currently unallocated resources, IT would aim to include these in the Fiscal Year 25-26 budget process and implement within that timeframe, if and as directed by the Board of Supervisors.

F6: Important Cyber Security projects and initiatives have not begun or are lagging due to insufficient staffing.

Response to F6:

The Board agrees with this finding. Mono County takes cybersecurity seriously and fosters a culture of cybersecurity awareness. While cybersecurity is ultimately the primary responsibility of each individual user in the environment, IT creates and implements policies to encourage a culture of individual concern and responsibility for maintaining cybersecurity. However, IT is currently in the process of staffing up following a series of departures.

Implementation of F6:

In March 2025, IT hired a Chief Information Security Officer. IT will work with Human Resources to develop a job description, determine the appropriate compensation and benefits, and recruit for a Cyber Security Analyst.

Implementation Timeline for F6*:*

The Board expects that IT will include the Cyber Security Analyst in its Fiscal Year 25-26 budget requests.

F7: Quarterly cyber security training is taking place with noteworthy results. However, there's a lack of visibility to compliance measurements among County executives.

Response to F7:

The Board agrees with this finding. Historically results of quarterly compliance trainings have not been brought to the Board of Supervisors. Some compliance issues also have not been brought to the Board because discussion of those items in open session may present security concerns.

Implementation of F7:

The Board of Supervisors will direct Mono County IT to create a standing quarterly agenda item to report out to the Board of Supervisors the results of training. IT will make recommendations to and take direction from the Board on the level of detail and information to be included in those reports.

IT will also begin reporting quarterly compliance to individual department heads for their department employees so that they have visibility.

Now that the legislature has passed an amendment allowing for cybersecurity threats and issues to be discussed in closed session under the Brown Act, the Board expects IT to bring closed session items as appropriate to discuss particular vulnerabilities identified during cyber security training.

Implementation Timeline for F7:

IT will make the first of these such reports to the Board and department heads in the first quarter of Fiscal Year 25-26.

Recommendations:

R2: The grand jury recommends the Board of Supervisors instruct the Director of Finance and Director of IT to document and put into practice a cooperative process for completing the annual PCI Compliance assessment. Recommendation to be completed by 08/01/2025.

Response to R2:

The Board agrees in part and disagrees in part with this recommendation.

Implementation of R2:

IT will train staff to be aware of PCI and SAQ requirements in order to better assist other county departments. IT will work with Finance to identify the correct SAQ form to be used during the self-assessment process and will partner with Finance and other departments responsible for processing customer credit cards to complete the SAQ and will provide input where appropriate.

Implementation Timeline for R2:

The Board expects training and collaboration with Finance in Fiscal Year 25-26.

R3: The grand jury recommends the Board of Supervisors instruct the Director of Finance and Director of IT to determine the correct PCI SAQ form(s) to be used in the County's next annual PCI Compliance assessment and attestation. Recommendation to be completed by 08/01/2025.

Response to R3:

The Board agrees in part and disagrees in part with this recommendation. Other departments that are responsible for processing consumer credit card information should also be involved in the process to identify the correct SAQ together with IT and Finance.

Implementation of R3:

IT will work with Finance to identify the correct SAQ form to be used during the self-assessment process.

Implementation Timeline for R3:

IT will complete this recommendation before the close of Fiscal Year 25-26.

R4: The grand jury recommends the Board of Supervisors instruct the Director of IT to document a plan to implement immutable backups for operationally critical data. Plan to be documented by 9/01/2025.

Response to R4:

The Board agrees with this recommendation.

Implementation of R4:

IT will research available and practical immutable backups and the possible implementation strategies for Mono County's needs. In doing so, IT will seek input from and collaboration with departments to identify their most critical systems that require immutable backups. IT will also work to develop a procedure for the implementation of immutable backups that then meets departmental needs.

The Board expects to review as part of a future budget process that includes resources to support a plan for immutable backups..

Implementation Timeline for R4:

The Board will expect IT to include required resources for an immutable backups plan in its FY 25-26 requests.

R5: The grand jury recommends the Board of Supervisors instruct the Director of IT to define a sustainable annual process to remove or replace unsupported computing devices from the environment. Recommendation to be completed by 08/01/2025.

Response to R5:

The Board agrees with this recommendation.

Implementation of R5:

As budget has not always been adequate to replace all end of life and end of sale equipment, IT will update its procedures and monitor the costs of replacement equipment to make the ISF more effective going forward.

The Board will review any additional personnel resources, such as another Network Specialist position, during future budget processes and allocation adjustments so that IT can meet schedules for removal and installation of equipment on an annual basis moving forward.

Implementation Timeline for R5:

IT will complete these actions by the close of Fiscal Year 25-26.

R6: The grand jury recommends the Board of Supervisors instruct the Director of IT to define a sustainable process to conduct periodic external penetration tests and vulnerability scans. Recommendation to be completed by 09/01/2025.

Response to R6:

The Board agrees with this recommendation.

Implementation of R6:

IT will explore additional penetration testing strategies and vendor relationships and can set a schedule in the context of those relationships for periodic testing.

Implementation Timeline for R6:

As penetration testing requires currently unallocated resources, the Board expects to review requests in the Fiscal Year 25-26 budget process and that IT will implement strategies within that timeframe.

R7: The grand jury recommends the Board of Supervisors instruct the Director of IT to assess the staffing and capacity demands needed to reasonably support Information Technology's Cyber Security roadmap for the purpose of submitting such staffing in its next fiscal year budget. Recommendation to be completed by 10/01/2025.

Response to R7:

The Board agrees with this recommendation.

Implementation of R7:

The Board will direct IT to assess its staffing needs following a series of departures this year. IT will also work to create an allocation and job description for a Cyber Security Analyst to add to the IT team and other personnel resources required by these Recommendations.

Implementation Timeline for R7:

IT will include all required personnel-related budget requests in its Fiscal Year 26-27 proposals.

R8: The grand jury recommends the Board of Supervisors instruct the Director of IT to implement a process for providing the Board of Supervisors a quarterly report on employee compliance to cybersecurity training. Recommendation to be completed by 10/01/2025.

Response to R7:

The Board agrees with this recommendation.

Implementation of R8:

IT will bring quarterly reports in open session to the Board in line with the Fiscal Year quarters, as well as to individual department heads.

Implementation Timeline for R8:

IT will bring the first such report in the first quarter of Fiscal Year 25-26.