County of Orange

County Executive Office

August 25, 2020

Honorable Kirk H. Nakamura
Presiding Judge of the Superior Court of California
700 Civic Center Drive West
Santa Ana, CA 92701

Subject: Response to Grand Jury Report, "Orange County's Cybersecurity Preparedness"

Dear Judge Nakamura:

Per your request, and in accordance with Penal Code 933, please find the County of Orange response to the subject report as approved by the Board of Supervisors. The respondents are the Orange County Board of Supervisors and the County Executive Office.

If you have any questions, please contact Lala Oca Ragen of the County Executive Office at 714-834-7219.

Sincerely,

Frank Kim
County Executive Officer

Enclosure

cc: Orange County Grand Jury
Lala Oca Ragen, Assistant Deputy Chief Operating Officer, County Executive Office

Responses to Findings and Recommendations
2019-20 Grand Jury Report:

"Orange County's Cybersecurity Preparedness"

SUMMARY RESPONSE STATEMENT:

On June 25, 2020, the Grand Jury released a report entitled "Orange County's Cybersecurity Preparedness."' This report directed responses to findings and recommendations to the Orange County Board of Supervisors. The responses are below:

FINDINGS AND RESPONSES:

F1. **Some County departments are not submitting monthly vulnerability scan results of their computer devices to OCIT to be entered into the County's enterprise Governance, Risk Management, and Compliance platform, and are non-compliant with the County Vulnerability Management Policy.**

Response: **Agrees with the finding.**

F2. **Some County departments have not established or submitted procedures to ensure application of software security patches based upon the severity level of the vulnerability, and are non-compliant with the County Patch Management Policy.**

Response: **Agrees with the finding.**

F3. **Even though a number of County departments are not in compliance with the County's Vulnerability Management Policy or Patch Management Policy, there have been no requests or approvals for variances from these policies, per the requirements of the County's Variance Review and Approval Process Policy.**

Response: **Agrees with the finding.**

F4. **The County's most recent Vulnerability/Penetration Assessment, performed by independent consultants in June 2019, was deemed to be "Incomplete," as only a portion of the County's externally facing servers and internal networks were permitted to be evaluated. An incomplete vulnerability/penetration assessment increases the potential vulnerability of County information systems.**

Response: **Agrees with the finding.**

RECOMMENDATIONS AND RESPONSES:

R1. **All County departments, including those with elected heads, should be required to comply with the County's Vulnerability Management and Patch Management Policies, or request variances from them, per the County's Variance Review and Approval Process Policy. (F1-F3)**

Response: **The recommendation requires further analysis.** The County's central IT organization (OCIT) will continue to work with all departments to encourage full compliance. OCIT will take the following actions within the next six months to support and facilitate policy compliance:

1. OCIT will offer its expertise, services and support capabilities to educate and implement viable solutions or workarounds for departments to comply with policy expectations and Grand Jury recommendations.
2. OCIT will work with departments to identify and mitigate obstacles that are preventing compliance and provide and facilitate variance forms for those that cannot be rectified.
3. OCIT will continue to encourage departments to leverage existing OCIT and County tools to manage/reduce vulnerabilities and risks.

R2. **All external facing servers and internal networks from all County departments, including those with elected heads, should be required to be included in future County vulnerability/penetration assessments so that the cybersecurity assessments can be considered complete. (F4)**

Response: **The recommendation requires further analysis.** The annual vendor penetration test is scheduled for September 2020. OCIT is in the process of obtaining full participation from each department and will execute the following tasks within the next six months:

1. OCIT will make all efforts to educate and solicit participation in penetration testing.
2. OCIT will work with non-compliant departments to identify and mitigate obstacles that are preventing compliance and/or develop variance forms for those that cannot be rectified.
3. OCT will request a scoping document from all departments to include the range of internal/external IP addresses that require scanning.