Orange County's Cybersecurity Preparedness

GRAND JURY 2019-2020

TABLE OF CONTENTS

SUMMARY

The 2019-2020 Grand Jury's investigation into the state of Orange County's cybersecurity preparedness focused on the review of a number of County provided cybersecurity reports, documents, policies and assessments related to the County's cybersecurity efforts. Potential threats in the cybersecurity landscape are ever evolving, and it is imperative that the County ensure compliance with its adopted policies across all County departments and continue to evaluate and implement new measures into their cybersecurity protocols and procedures.

The Grand Jury's investigation revealed that some County departments are currently out of compliance with the County's Vulnerability and Patch Management Policies, and there have been no approvals for variances from these policies as required by the County's Variance Review and Approval Process Policy.

A review of the County's most recent Vulnerability/Penetration Assessment, performed by independent IT consultants in June 2019, concluded that the top priority for the County's cybersecurity efforts should be to update software across the County's IT systems to remove or mitigate thousands of existing serious security vulnerabilities. This cybersecurity assessment was also deemed by the consultants to be "Incomplete" in that 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 to cyberattacks for County information systems and data.

The Grand Jury believes that the County has the oversight responsibility and liability for the county-owned computer systems and data residing within all County departments, including those headed by elected officials, and that the County should require all County departments to comply with its cybersecurity policies and participate in vulnerability and penetration assessments.

REASON FOR THE STUDY

The security of Orange County's information technology systems and data are of vital importance to the functioning of the County's government and services. The ability to protect the County from cyberattacks and sustain essential functions is the foundation of a resilient cybersecurity program. A review of the Grand Jury's 2016-2017 report on the status of County cybersecurity revealed that many of the report's recommended actions were just being implemented, three years later. The reason for the 2019-2020 Orange County Grand Jury's investigation was to assess the current status of the County's cybersecurity preparedness, policies and procedures, and recommend actions which could improve the County's cybersecurity resilience.

METHOD OF STUDY

In conducting its investigation, the Grand Jury reviewed numerous County-produced cybersecurity reports, policies, documents, and assessments, as well as online research. The Grand Jury interviewed six County employees and an IT consulting contractor to the County. Much of the information and reports which were reviewed and relied on were provided by Orange County Information Technology (OCIT) and contained non-public and potentially sensitive information.

Due to the COVID-19 pandemic, the 2019-2020 Grand Jury was required to suspend its investigation for almost nine weeks. Unfortunately, this limited the Grand Jury's time to complete the investigation, including receiving and reviewing additional requested information from OCIT regarding policy compliance updates, and additional interviews of IT personnel from some departments.

BACKGROUND AND FACTS

Introduction

The 2019-2020 Grand Jury's investigation into the state of the County's cybersecurity preparedness focused on the review of a number of reports and documents related to the County's cybersecurity preparedness including the following;

- The 2016-2017 Orange County Grand Jury's report on Digital Data
- The County's two most recent State of County Cybersecurity reports
- The County's Cybersecurity Best Practices Manual
- The County's Cybersecurity Policy (Draft)
- Individual County policies related to cybersecurity
- June 2019 Security Architecture and Vulnerability/Penetration Assessment

Following is a brief discussion of each of these reports and documents, including information which is considered pertinent to the Grand Jury's investigation, findings and recommendations.

2016-2017 Orange County Grand Jury Report on Digital Data

The 2016-2017 Orange County Grand Jury's report entitled "Orange County's Digital Data: Is it Protected from Cyber Attack?" contained numerous findings and recommendations on enhancing the County's cybersecurity preparedness. Responses to the report's recommendations from the County were received in September 2017, with additional follow-up responses in March 2018. Many of the report's recommendations have been adopted and implemented by the County and Orange County Information Technology (OCIT).

Of the report's recommendations, two in particular were considered relevant to the Grand Jury's current investigation. These two recommendations and the County's responses, are set out as follows:

1. **Recommendation 15**: Procedures for updating and patching all County software and systems that have been established by OCIT for the shared services program should be made mandatory for all County departments and agencies that report to the CEO, and recommended for all other county government entities by 6/30/2018.

   County Response in Sept 2017: This recommendation has not yet been implemented but will be in the future. OCIT has procured vulnerability scanning software and implemented network architecture to enable supporting other County departments with the conduct of vulnerability scans. These scans are used to determine the level of

patching required for County information systems and networks. Most departments are already doing automated patching of systems and software; the only component missing is the vulnerability scanning for verification. This issue will be resolved as part of the technical controls to be implemented through the efforts of the Cyber Security Joint Task Force (CSJTF).

County Follow up Response in March 2018: OCIT has initiated vulnerability scanning for county departments and tracks findings in the County Governance, Risk, and Compliance Platform. This practice is included in the technical controls that will be submitted to the CSJTF for approval. Vulnerability scanning is a key component for the development of a County Security Operations Center.

Recommendation 18: OCIT should establish standardized procedures for conducting periodic cybersecurity vulnerability and penetration testing by 12/31/19.

County Response from Sept 2017: This recommendation has been implemented. This process is implemented and is currently being realized through the countywide cyber security audits and assessments. Additionally, OCIT oversees the conduct of a penetration test of the County externally facing network systems and security appliances. Part of this annual penetration testing is also to conduct a comprehensive vulnerability scan and social engineering penetration test. Social Engineering is the act of manipulating an employee into providing access to county information systems and networks through either a phishing attempt, phone scams and or other means of contacting the target of the attack. Penetration testing services are also offered under the Tevora RCA for audit and assessment services.

It is noted that the Cybersecurity Joint Task Force (CSJTF) is a committee formed to oversee County cybersecurity policy development, and to insure that county assets and systems are as safe as practicable now and into the future. The Cybersecurity Joint Task Force (CSJTF) is comprised of representatives from County Risk Management, Departmental Administrative Services, and Departmental Information Technology, and is chaired by the County Chief Information Security Officer (CISO). The purpose of the CSJTF task force is to develop and oversee compliance with the County Cybersecurity Manual, which establishes a common set of standards and practices to improve the Cybersecurity posture for all County departments.

In 2018, OCIT procured a software platform for its Governance, Risk Management & Compliance (GRC) initiative. The GRC provides a central location for assessment results from throughout the county. This information along with controls, drives actions that will mitigate

cyber threats. The GRC platform is used to track individual findings and vulnerabilities that can be followed down to a specific location. This results in a disciplined and efficient approach to remediation of cybersecurity deficiencies, whether they are technical in nature or administrative.[1]

The potential threats in the cybersecurity landscape are ever-evolving, and it is imperative that the County ensure compliance with its adopted policies across all County departments, and continue to evaluate and implement new measures to their cybersecurity protocols and procedures.

State of County Cybersecurity Reports

A review was made of the two most recent State of County Cybersecurity reports prepared by Orange County Information Technology (OCIT), dated June 2018 and December 2019. These reports were requested from OCIT by the Board of Supervisors to provide an update on the state of the County's cybersecurity preparedness.

The December 2019 report indicates that OCIT is responsible for approximately seventy-five percent of the County's cyber preparedness program. While OCIT collaborates and assists in various ways with the remaining twenty-five percent of the County, they state that they realistically cannot certify that the County fully complies with the cyber preparedness program across all County departments. OCIT recommends in its report that the Board of Supervisors initiate steps to consolidate all technology infrastructure across all County departments.

The 2019 State of County Privacy and Cybersecurity report also identifies some of OCIT's recent cybersecurity efforts. OCIT has deployed an enterprise solution for vulnerability scanning which is available to all County departments. The objective of the vulnerability management program is to reduce the time that a vulnerability is exposed to threats.

The 2019 report also indicates that updating and patching of software is fundamental to effective cybersecurity hygiene and is critical for mitigation of risks related to ransomware exploitation. Rapid remediation of identified vulnerabilities with minimal user intervention is critical for large enterprises such as the County. OCIT recommends that the County acquire automated patching software tools to enhance its cybersecurity program. Continued follow-up and process improvement is critical to ensuring that the standards established in the County's Vulnerability and Patch Management Policies are adhered to across all County departments.

[1] State of County Cybersecurity Bi-Annual Report, June 2018

County's Cybersecurity Best Practices Manual

The County's Cybersecurity Best Practices Manual was prepared by the Cyber Security Joint Task Force and approved by the IT Executive Council at its August 2018 meeting. This manual provides a framework and describes best practices to establish a secure environment that safeguards the confidentiality, integrity and availability of the data and information systems used to manage the services provided by the County. The Cybersecurity Best Practices Manual applies to all departments in the County.

To maintain a strong cybersecurity posture it is essential for cybersecurity programs to include procedures and controls implemented within all departments to secure data and information systems. Each department is required to develop a departmental cybersecurity program, with the procedures and controls included in the departmental program to be determined by the department. The Cybersecurity Best Practices Manual is intended to provide guidelines for departments, and any changes or modifications to the guidelines need to be discussed with OCIT.

County Cybersecurity Policy

The County has recently developed an overall County Cybersecurity Policy in order to provide guidance and protection to County employees, and to safeguard the information resources entrusted to employees. The County's Cybersecurity Policy is based upon NIST SP 800-53 standards and best practices, and is considered the minimum standard for providing a secure environment. The County Cybersecurity Policy was approved and adopted by the CSJTF in August 2019. Although OCIT believes that passage of the Policy is the correct step, the CSJTF vote was not unanimous. The Policy recently passed a vote of the IT Executive Council, and as of the publication of this report is in the process of being approved and adopted by the County CEO.

Following is a summary of some of the pertinent components of the County Cybersecurity Policy:

- **Approval/Revision Dates**: Approved by CSJTF on August 8, 2019, pending approval by IT Executive Council and CEO
- **Authority:** County Executive Office
- **Policy Owner:** County Chief Information Officer
- **Policy:** Departments shall develop, implement, and maintain a Cybersecurity program that consists of policies, procedures, plans, and guidelines for safeguards to protect information during storage, use or in transit.

- **Scop**e: This policy applies to all departments in the County as well as all employees, contractors, vendors, customers, and others who utilize, possess or have access to County IT resources.
- **Compliance:** The County shall verify compliance with this policy.
- **Variances:** Variances to this policy shall be documented and approved following the County Variance Review and Approval Process.
- **Non-Compliance:** Non-compliance with this policy may result in significant delays to the implementation of information systems and/or technologies. Devices not in compliance with the Policy may have their access to the County's network restricted.
- **Policy Control and Maintenance:** The County Chief Information Security Officer is responsible for maintaining this policy.

County Vulnerability Management Policy

A vulnerability management process identifies, analyzes and manages vulnerabilities in an organization's operating environment. The vulnerability management process is divided into three areas:

> Vulnerability Management – lays the foundation for the Vulnerability Management Program and establishes the management framework for monitoring, mitigating and preventing future vulnerabilities to County assets.
>
> Vulnerability Monitoring – commonly employs tools and process capable of detecting and determining various types of vulnerabilities and determining remediation and mitigation strategies.
>
> Vulnerability Remediation and Mitigation – involves the analysis of risk from identified vulnerabilities, prioritizing those vulnerabilities and determining remediation and mitigation strategies.

As part of its vulnerability management program, the County adopted a Vulnerability Management Policy in August 2018. Following is a summary of its pertinent components:

- **Approval/Revision Dates**: Approved 8/15/2018, No Revisions
- **Authority:** County Executive Office
- **Policy Owner:** County Chief Information Officer
- **Policy:** Each Department shall develop and maintain a Vulnerability Management process as part of its Cybersecurity program, and shall perform monthly vulnerability scans with the results entered into the County enterprise GRC platform.

- **Scope**: This policy applies to all County departments.
- **Compliance:** An entity designated by the County shall verify compliance to this policy through various methods including internal and external audits.
- **Variances:** Variances to this policy shall be documented and approved following the County Variance Review and Approval Process.
- **Non-Compliance:** Non-compliance with this policy may result in unidentified vulnerabilities that compromise County data and/or assets
- **Policy Control and Maintenance:** The County Chief Information Security Officer is responsible for maintaining this policy.

OCIT has deployed an enterprise solution for vulnerability scanning which is available to all County departments. OCIT advised the Grand Jury that while most County departments are currently participating and utilizing this vulnerability scanning software, some departments may be utilizing other software and have not provided scanning results to OCIT on a monthly basis to be in compliance with the Vulnerability Management Policy. OCIT advised the Grand Jury that the departments which are currently not submitting vulnerability scan results include the Auditor/Controller, Treasurer/Tax Collector, Health Care Agency, Sheriff/Coroner, District Attorney, and Public Defender.

While the Grand Jury has been informed by County executives that they do not have the authority to instruct elected officials on how to operate their departments, the Grand Jury believes the County has the oversight responsibility and liability for the County Policies pertaining to the County owned computer systems and data residing within all County departments, including those headed by elected officials. The Grand Jury believes that the County needs to do more than recommend compliance to departments with elected officials, and should require all County departments to comply with its cybersecurity policies, including this Vulnerability Management Policy. In-lieu of participating in the County's monthly vulnerability scanning, a department could choose to comply by performing their own vulnerability scans and providing the results to the County Governance, Risk and Compliance platform.

County Patch Management Policy

Patch management has emerged as one of the more critical issues for today's IT organizations. The importance of efficient application of vendor-supplied patches cannot be understated, particularly in light of increasing vulnerability alerts, intrusion activity, and virus proliferation. Vulnerabilities arising from unpatched or misconfigured software account for the majority of all internet security breaches.

Patch management is integral to a department's cybersecurity program, in particular its vulnerability management program. Responsible IT organizations have an obligation to establish assertive, systematic patch management processes based upon a solid foundation of policy, procedures and training. Failure in doing so is to court risk and invite disruption of business activity.

As part of its cybersecurity program, the County adopted a Patch Management Policy in August 2018. Following is a summary of its pertinent components:

- **Approval/Revision Dates**: Approved 1/28/2004, Revised 8/15/2018
- **Authority:** County Executive Office
- **Policy Owner:** County Chief Information Officer
- **Policy:** County departments shall establish internal processes and procedures to ensure efficient application of vendor-supplied security patches based upon the severity level of the vulnerabilities identified.
- **Scop**e: This policy applies to all County departments.
- **Compliance:** An entity designated by the County shall verify compliance to this policy through various methods including internal and external audits.
- **Variances:** Variances to this policy shall be documented and approved following the County Variance Review and Approval Process.
- **Non-Compliance:** Non-compliance with this policy may result in vulnerabilities that compromise County data and/or assets. Devices not in compliance with this policy may have their access to the County's network restricted.
- **Policy Control and Maintenance:** The County Chief Information Security Officer is responsible for maintaining this policy.

OCIT advised the Grand Jury that while most County departments are currently participating and have established internal processes and procedures to ensure efficient application of vendor supplied security patches, some departments have not, and are not in compliance with the Patch Management Policy. The Grand Jury requested the status of compliance for each department with the Patch Management Policy from OCIT, however this information was not received prior to the publication of this report.

Reiterated from the discussion on the prior policy, the Grand Jury believes that the County has the oversight responsibility and liability for County Policies pertaining to the County owned computer systems and data residing within all County departments, including those headed by elected officials. The Grand Jury believes that the County needs to do more than recommend compliance to departments with elected officials, and should require all County departments to

comply with its policies related to cybersecurity, including this Patch Management policy establishing internal processes and procedures to ensure efficient application of vendor-supplied security patches.

County Cyber Incident Reporting Policy

As part of its cybersecurity program, the County adopted a Cyber Incident Reporting Policy in September 2018. The County Cyber Incident Reporting Policy seeks to ensure that the Board of Supervisors, County Executive Office, and impacted Department Heads are informed of significant cybersecurity incidents in a timely manner.

Following is a summary of the pertinent components of the Cyber Incident Reporting Policy:

- **Approval/Revision Dates**: Approved 9/26/2018, No Revisions
- **Authority:** County Executive Office
- **Policy Owner:** County Chief Information Officer
- **Policy:** County departments shall report cybersecurity incidents to the Central IT Service Desk. Confirmed cybersecurity incidents that meet the criteria defined in the Significant Incident/Claim Reporting Protocol shall be reported by the CISO to the CIO, CEO, and the Board of Supervisors within 24 hours. County departments shall review and confirm the accuracy of the Confirmed Cybersecurity Incident Report prepared by OCIT annually.
- **Scop**e: This policy applies to all County departments.
- **Compliance:** The County shall verify compliance to this policy including internal and external audits.
- **Variances:** Variances to this policy shall be documented and approved following the County Variance Review and Approval Process.
- **Non-Compliance:** Non-compliance with this policy may result in cybersecurity incidents not being properly reported and addressed.
- **Policy Control and Maintenance:** The County Chief Information Security Officer is responsible for maintaining this policy.
- **Reporting Criteria:** The CISO shall report to the Board of Supervisors any confirmed cybersecurity incident that meets any of the following criteria:
    - Involves a natural disaster or other incident that impact County residents and property
    - Involves an unusual or significant dangerous condition of property that is owned, occupied or maintained by the County
    - Involves sensitive issues of government practices or public policy

- Involves multiple cities or jurisdictions and will require coordination with cities, state agencies/departments, and or the federal government
- Involves reports from County contracted consultants or a government agency critical of County policy, procedure or processes
- Has the potential to result in a claim/litigation against the County
- May attract significant media attention

It is imperative to County decision-makers and residents that significant cyber incidents which occur on County IT systems and networks be reported to the County CIO, CEO, and Board of Supervisors within 24 hours. OCIT indicated that as of January 2020, there have been no confirmed cybersecurity incidents reported to them which meet the criteria defined in the Significant Incident/Claim Reporting. The Grand Jury requested documentation from OCIT confirming compliance with this County Policy, however this information was not received prior to the completion of its investigation.

County Variance Review and Approval Process Policy

The County Policy for Variance Review and Approval Process allows for Department heads and County leadership to make an informed decision on whether or not to accept a variance from the Cybersecurity Best Practices Manual or County policies by understanding the risks and alternatives involved. All requests for variances are to be documented using the County Variance Request Form and are to be logged in a central repository, to be maintained by OCIT. Approved County Variance Request Forms shall be reviewed at least annually for renewal by the CISO and the department requesting the variance.

Following is a summary of the pertinent components of the Variance Review and Approval Process Policy:

- **Approval/Revision Dates**: Approved 4/2/2018, No Revisions
- **Authority:** County Executive Office
- **Policy Owner:** County Chief Information Officer
- **Policy:** The procedure will allow department heads and County leadership to make an informed decision on whether or not to accept a variance from the Cybersecurity Manual or County Policy by understanding the risks and alternatives involved.
- **Scop**e: This procedure applies to all departments in the County.
- **Compliance:** An entity designated by the County shall verify compliance to this policy through various methods including internal and external audits.
- **Variances:** Variances to this policy shall be documented and approved following the County Variance Review and Approval Process.

- **Non-Compliance:** Non-compliance with this policy may result in significant delays to the implementation of information systems and/or technologies.
- **Policy Control and Maintenance:** The County Chief Information Security Officer is responsible for maintaining this policy.

A review of the current repository of all requested variances indicates that only four requests for variances have been received as of February 2020. A summary of the four variance requests is set out below:

1. August 2018 – Use of Administrative Accounts by system administrators
2. August 2019 – ROV Windows 2000 Plate Printers
3. February 2019 – OCCR Public Library Network Traffic Monitoring
4. February 2019 - Clerk of the Board Desktop Admin Account

While the total number of existing issues requiring variances from the County's cybersecurity best practices and policies is unknown, it is apparent that many non-compliant issues currently exist. It is imperative that all County departments comply with the County's adopted cybersecurity best practices and policies or submit the required requests for variances.

Security Architecture and Vulnerability/Penetration Assessment

As part of the Grand Jury's investigation into the County's cybersecurity preparedness, a review was made of the most recent Security Architecture and Vulnerability/Penetration Assessment, dated July 12, 2019, which was conducted by IT consultants retained by the County.

The Security Architecture Assessment compared the capabilities of the security tools deployed by the County, as well as the security process used by the County, with an appropriate set of security controls derived from the NIST 800-53 Standard. The results of this assessment provide the OCIT Security organization with a prioritized list of initiatives to implement new or different security tools or security processes. These initiatives can better equip the County of Orange to proactively combat the growing cybersecurity attacks causing data breaches and millions of dollars of potential ransomware.

The External and Internal Security Assessments assessed the vulnerability of selected external and internal computing and network devices of the County. The IT consultant deployed several automated tools and utilized techniques in order to evaluate the vulnerability of servers, workstations and networking devices to a cybersecurity attack across the public internet, or origination from within the County's internal networks.

Based on the results of the Security Architecture Assessment, the County's existing security controls can provide the majority of the security controls that the County should have in place, but there are several significant gaps in controls that need to be addressed. The two most significant findings of this assessment were that many of the County's external and internal hosts are running out-of-date software, and that numerous departments/agencies chose not to participate and therefore the assessment was deemed by the consultants to be "Incomplete." The assessment also concluded that because of the prevalence of out-of-support and unpatched software in the County's environment, the County is at "high risk" of being compromised by a cyberattack.

While the Grand Jury has been informed by County executives that they do not have the authority to direct elected officials on how to operate their departments, the Grand Jury believes the County has the responsibility and liability for the County owned computer systems and data residing within all County departments, including those headed by elected officials. It is recognized that penetration testing assessments can be disruptive and interfere with regular business operations. However, the County's IT consultant who performed the most recent assessment has indicated that a penetration assessment could be conducted during off-business times and terms acceptable to individual department's IT needs and security requirements.

The Grand Jury believes that the County needs to do more than recommend participation in future County-wide vulnerability/penetration assessments, and should require all external facing servers and internal networks from all County departments to be included. In-lieu of participating in the County conducted vulnerability/penetration assessment, a department could choose to comply by performing its own vulnerability/penetration assessments and provide the results to the County, as long as the criteria for the assessment is equal to or exceeds County standards.

FINDINGS

Pursuant to California Penal Code Sections 933 and 933.05, the Grand Jury requires (or, as noted, requests) responses from each agency affected by the findings presented in this section. The responses are to be submitted to the Presiding Judge of the Superior Court.

Based on its investigation entitled "Orange County's Cybersecurity Preparedness," the 2019-2020 Orange County Grand Jury has arrived at four principal findings as follows:

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.

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.

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.

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.

RECOMMENDATIONS

In accordance with California Penal Code Sections §933 and §933.05, the 2019-2020 Grand Jury requires responses from each agency affected by the recommendations presented in this section. The responses are to be submitted to the Presiding Judge of the Superior Court.

Based on its investigation described here, the 2019-2020 Orange County Grand Jury has arrived at the following recommendations:

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)

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)

RESPONSES

The following excerpts from the California Penal Code provide the requirements for public agencies to respond to the findings and recommendations of this Grand Jury report:

§933 "Comments and Reports on Grand Jury Recommendations."

"(c) No later than 90 days after the grand jury submits a final report on the operations of any public agency subject to its reviewing authority, the governing body of the public agency shall comment to the presiding judge of the superior court on the findings and recommendations pertaining to matters under the control of the governing body and every elected county officer or agency head for which the grand jury has responsibility pursuant to Section 914.1 shall comment within 60 days to the presiding judge of the superior court, with an information copy sent to the board of supervisors, on the findings and recommendations pertaining to matters under the control of that county officer or agency head or any agency or agencies which that officer or agency head supervises or controls. In any city and county, the mayor shall also comment on the findings and recommendations. All of these comments and reports shall forthwith be submitted to the presiding judge of the superior court who impaneled the grand jury. A copy of all responses to grand jury reports shall be placed on file with the clerk of the public agency and the office of the county clerk, or the mayor when applicable, and shall remain on file in those offices...."

§933.05 "Response to Grand Jury Recommendations – Content Requirements; Personal Appearances by Responding Party; Grand Jury Report to Affected Agency."

"(a) For purposes of subdivision (b) of Section 933, as to each grand jury finding, the responding person or entity shall indicate one of the following:

(1) The respondent agrees with the finding.

(2) The respondent disagrees wholly or partially with the finding, in which case the response shall specify the portion of the finding that is disputed and shall include an explanation of the reasons therefor.

(b) For purposes of subdivision (b) of Section 933, as to each grand jury recommendation, the responding person or entity shall report one of the following actions:

(1) The recommendation has been implemented, with a summary regarding the implemented action.

(2) The recommendation has not yet been implemented, but will be implemented in the future, with a timeframe for implementation.

(3) The recommendation requires further analysis, with an explanation and the scope and parameters of an analysis or study, and a timeframe for the matter to be prepared for discussion by the officer or head of the agency or department being investigated or reviewed, including the governing body of the public agency when applicable. This timeframe shall not exceed six months from the date of publication of the grand jury report.

(4) The recommendation will not be implemented because it is not warranted or is not reasonable, with an explanation therefor.

(c) However, if a finding or recommendation of the Grand Jury addresses budgetary or personnel matters of a county agency or department headed by an elected officer, both the agency or department head and the board of supervisors shall respond if requested by the grand jury, but the response of the board of supervisors shall address only those budgetary or personnel matters over which it has some decision-making authority. The response of the elected agency or department head shall address all aspects of the findings or recommendations affecting his or her agency or department."

Responses Required

Comments to the Presiding Judge of the Superior Court in compliance with California Penal Code Section 933.5 are required from:

Findings

County of Orange Board of Supervisors	F1-F4

Recommendations

County of Orange Board of Supervisors	R1, R2

REFERENCES

- NIST SP 800-53 standards (National Institute of Standards and Technology)
- County of Orange Cybersecurity Best Practices Manual prepared by the Cybersecurity Joint Task Force and approved by the IT Executive Council August 21, 2018.

GLOSSARY

A list of definitions for acronyms is included here:

OCIT	Orange County Information Technology
CSJTF	The Cybersecurity Joint Task Force
CISO	County Chief Information Security Officer
CIO	Chief Information Officer
CEO	Chief Executive Officer
ROV	Registrar of Voters
OCCR	Orange County Community Resources