# County of Orange

County Executive Office

September 12, 2017

Honorable Charles Margines
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 Digital Data: Is It Protected From Cyber Attack?"

Dear Judge Margines:

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

If you have any questions, please contact Lilly Simmering of the County Executive Office at 714-834-6748.

Sincerely,

Frank Kim
County Executive Officer

Enclosure

cc: FY 2016-17 Orange County Grand Jury Foreman
Lilly Simmering, Deputy Chief Operating Officer, County Executive Office

Agenda Item 34

# AGENDA STAFF REPORT

ASR Control 17-000984

| | |
|---|---|
| **MEETING DATE:** | 09/12/17 |
| **LEGAL ENTITY TAKING ACTION:** | Board of Supervisors |
| **BOARD OF SUPERVISORS DISTRICT(S):** | All Districts |
| **SUBMITTING AGENCY/DEPARTMENT:** | County Executive Office (Approved) |
| **DEPARTMENT CONTACT PERSON(S):** | Joel Golub (714) 834 6287 |
| | Lilly Simmering (714) 834 6748 |



**SUBJECT:** Orange County's Digital Data Grand Jury Response

| CEO CONCUR | COUNTY COUNSEL REVIEW | CLERK OF THE BOARD |
|---|---|---|
| Concur | No Legal Objection | Discussion<br>3 Votes Board Majority |

**Budgeted:** N/A **Current Year Cost:** N/A **Annual Cost:** N/A

**Staffing Impact:** No **# of Positions:** **Sole Source:** N/A

**Current Fiscal Year Revenue:** N/A

**Funding Source:** N/A **County Audit in last 3 years:** No

**Prior Board Action:** N/A

## RECOMMENDED ACTION(S):

1. Approve proposed response to FY 2016-17 Grand Jury Report entitled, "Orange County's Digital Data: Is it Protected from Cyber Attack?"
2. Direct the Clerk of the Board to forward this Agenda Staff Report with attachments to the Presiding Judge of the Superior Court and the FY 2016-17 Grand Jury no later than September 19, 2017.

## SUMMARY:

Approval of proposed response to FY 2016-17 Grand Jury Report entitled, "Orange County's Digital Data: Is it Protected from Cyber Attack?" will fulfill the County's required response to the Grand Jury.

## BACKGROUND INFORMATION:

On June 29, 2017, the Orange County Grand Jury released a report entitled, "Orange County's Digital Data: Is it Protected from Cyber Attack?" The report directed responses to findings and recommendations to the Orange County Board of Supervisors, the County Executive Office, and the Orange County Office

of Information Technology. Attachment B is the County's proposed response to the Grand Jury's findings and recommendations.

**FINANCIAL IMPACT:**

N/A

**STAFFING IMPACT:**

N/A

**ATTACHMENT(S):**

Attachment A - Report, "Orange County's Digital Data: Is it Protected from Cyber Attack?"
Attachment B - Proposed Responses to Findings and Recommendations
Attachment C - Draft Transmittal Letter

**Responses to Findings and Recommendations**
**2016-17 Grand Jury Report:**

***"Orange County's Digital Data: Is It Protected From Cyber Attack?"***

---

SUMMARY RESPONSE STATEMENT:

On June 29, 2017 the Grand Jury released a report entitled: "Orange County's Digital Data: Is It Protected From Cyber Attack?" This report directed responses to findings and recommendations to the Orange County Board of Supervisors, the County Executive Office, and the Orange County Office of Information Technology, which are included below.

FINDINGS AND RESPONSES:

**F.1.** **Orange County government entities are prime cyber targets, under constant cyber attack, and both public and private information held by these entities are not adequately protected.**

**Response:** **Disagrees partially with this finding.** Orange County is no more a target than other government agencies. Government agencies are continuously targeted for various reasons such as hacktivism and cyber crime. It is not correct to say the information is not adequately protected. Information systems are protected and monitored. Orange County has a robust Cyber Security Deterrence Program. Continuous improvement in this area is being addressed by way of county wide cyber security assessments and the establishment of a County Cyber Security Joint Task Force (CSJTF). The CSJTF was established to standardize security controls and methodologies across all County departments.

**F.2.** **The county is subject to many types of cyber attacks but phishing currently represents the highest risk to the county's sensitive information.**

**Response:** **Agrees with this finding.**

**F.3.** **Some county cyber attacks come through third-party vendors, who may not always be sufficiently protected.**

**Response:** **Agrees with this finding.** Third party vendors are now vetted for their security protocols during the procurement cycle and when third party vendors "enter" the County's network, they are subject to County standards.

**F.4.** **The county has taken a number of steps to safeguard its digital data and systems against cyber attack, but there are a number of actions generally recognized as cybersecurity best practices that still need to be implemented.**

**Response:** **Partially disagrees with this finding.** As mentioned earlier, cybersecurity measures are ever evolving; which best practices the County will choose to implement will be based on County-specific evaluations. The Board of Supervisors has authorized a dedicated team to lead county security planning, deployment and recovery. The County adheres to best practice both in the commercial and government space and continues to evaluate changes to our protocols as new measures are available.

**F.5.** **County financial records do not separate out cybersecurity as a line item, making it hard to determine what resources are being allocated in the area and therefore what additional funds are needed.**

**Response:** **Disagrees with this finding.** OCIT maintains an Enterprise Security budget which is meant to cover cyber security management, maintenance, assessment, incident response, and new initiatives.

**F.6.** **Cooperation among county agencies is currently limited due to organizational and cultural issues including the visibility of available centralized OCIT cybersecurity support, the inward focus of county agencies and the fact that the influence of the BOS to compel collaboration is largely limited to county agencies with appointed heads that report to the county CEO and, to a lesser degree, the county agencies with elected heads.**

**Response:** **Respondent disagrees with this finding.** The CJSTF represents a major shift in this culture as it is made up of representatives from all County departments, including elected and appointed departments. Additionally, both elected and non-elected department heads sit on the IT Executive Council – a Board of Supervisors-approved IT governance body. OCIT Enterprise Security has seen an increased interest over the past 18 months in sharing information and improved collaboration in the areas of mitigating risks of cyber threats and responding to cyber security incidents. Departmental leadership understands the County is stronger when all departments collaborate to reduce the risks associated with cyber threats as evidenced by the participation on the CSJTF and the IT Executive Council.

**F.7.** **OCIT has an effective team in place for addressing cybersecurity deficiencies, but it is only in the formative stages of implementing centralized standards and best practices for cybersecurity. Outside OCIT's control, county government agencies are taking advantage of the county's cybersecurity initiatives to different degrees.**

**Response:** **Agrees with this finding.**

F.8. **IT employees across county government are largely untrained and uncertified in cybersecurity, especially at the agency level. Staffing for cybersecurity is challenging due to outdated county cybersecurity job classifications and salary levels, as well as lengthy county hiring processes, particularly for those agencies requiring extensive background checks.**

**Response:** **Disagrees partially with this finding.** Some departments do provide security specific training such as the County's Health Care Agency. OCIT Enterprise Security is addressing this issue, by increasing the IT security training budget from $30,000 to $50,000 annually. With respect to non-IT employees, the County implemented mandatory online Cyber Security Awareness Training (CSAT) in January of 2017. Since implementation, over 90% of County employees have competed the online CSAT. The CISO agrees with the finding that it is challenging to hire cyber security professionals for the reasons stated in this finding.

RECOMMENDATIONS AND RESPONSES:

R.1. **The county should review, update and standardize all employee and contractor exit procedures to ensure the security of the countywide sensitive information by 12/31/2017.**

**Response:** **The recommendation has not yet been implemented but it will be implemented.** The recommendation will be implemented through the CSJTF and the publishing of the County Cyber Security Policy and Process Manual. By charter, the CSJTF is not due to provide the IT Executive Council the final product for approval until March 30, 2018.

R.2. **OCIT should select, acquire and direct the implementation of computer-based data loss prevention capability by 12/31/2017.**

**Response:** **This recommendation has been implemented.** OCIT has begun the process of implementing county-wide Data Loss Prevention (DLP) through our email system. The policies are designed to prevent transmission of sensitive information such as credit card information, personally identifiable information (PII) and health record information. The County Privacy Officer is leading the effort to develop the DLP policies in collaboration with County departments.

R.3. **The county should review, update and standardize all employee and contractor exit procedures to ensure the security of countywide sensitive information by 12/31/2017.**

**Response:** **This recommendation requires further analysis.** Access control reviews are currently underway as part of the countywide cyber security assessments. Review of access controls determines the individuals with access to data and systems and whether there is still a need to have access to said data and systems. The County is expected to have all departments complete these cyber security assessments by June 8, 2018.

R.4. **OCIT should establish a countywide cybersecurity working group by 12/31/2017. Participation should be mandatory for County of Orange agencies that report to the CEO and highly recommended for other county government entities.**

**Response:** **This recommendation has been implemented.** The CJSTF serves as the working group for cyber security.

R.5. **OCIT should develop a formal five-year cybersecurity strategic plan as a separate part of the IT Strategic Plan in the next county strategic plan.**

**Response:** **This recommendation has been implemented.** OCIT does have a formalized road map for Cyber Security to take the County to a point of maturity where the County is implementing National Institute of Standards and Technology (NIST) Cyber Security and Risk Management Frameworks (RMF) and other appropriate measures.

R.6. **OCIT should finalize a mandatory county incident response plan with procedures for individual agency exceptions and present it to the appropriate oversight bodies and BOS for approval by 7/1/2018.**

**Response:** **This recommendation has not yet been implemented but will be implemented in the future.** OCIT has developed and implemented a Cyber Incident Response Plan (CIRP) that has been tested. OCIT Enterprise Security plans to adopt the CIRP, through a vote of the CSJTF, prior to March 30, 2018.

R.7. **The county should include in its 2018-19 IT Strategic Plan the identification, documentation and categorization by risk of county digital sensitive information.**

**Response:** **This recommendation has not yet been implemented but it will be implemented in the future.** This issue is best addressed through a strategic level initiative to centralize management of data exfiltration points and establishment of a formal Data Classification Policy. The CJSTF is the strategic level mechanism that will address how sensitive digital information is to be classified and handled.

R.8. **The county should annually review and update the amount and types of county cyber insurance based on the annual county risk analysis.**

**Response:** **This recommendation has been implemented.** County Risk Management Office currently reviews and manages the cyber insurance policy for the County.

R.9. **OCIT should implement cybersecurity training and professional certification of all IT analysts having cybersecurity as a part of their job responsibilities by 7/1/2108.**

**Response:** **This recommendation requires further analysis.** While OCIT has an executed training program, the County cyber security assessments scheduled to be completed in June of 2018

will provide additional details about what trainings and certifications the departments will need. Until the departmental assessment reports are reviewed, it is not possible to provide any additional information or determine an approach to implementing this recommendation.

**R.10. OCIT should establish audit and test procedures to periodically, but no less than every two years, gauge the effectiveness of training and other cybersecurity measures by 7/1/2018.**

**Response: This recommendation has been implemented.** The County annually conducts the following evaluations as part of its contract with its enterprise network vendors: penetrations tests, social engineering tests, vulnerability assessments of the enterprise networks, and tests of the County disaster recovery site. Reports of findings from the annual penetration tests are provided to department IT directors and tracked for remediation by OCIT Enterprise Security. Additionally, on April 11, 2017, the Board of Supervisors approved a cooperative agreement with Tevora Business Solutions, Inc. for the purpose of affording County departments with accessibility to cyber security audit and assessment services. The Board of Supervisors further directed all County departments to complete a cyber security assessment not later than June of 2018. In addition, the CJSTF will be formalizing the periodic cyber security audit and assessment cycle as part of the County Cyber Security Policy and Process Manual.

**R.11. The county should establish separate budget line items for cybersecurity expenses and capital investments for the 2018-2019 budget.**

**Response: This recommendation has been implemented.** OCIT maintains an Enterprise Security budget which is meant to cover cyber security management, maintenance, assessment, and incident response.

**R.12. The county should implement the use of regional cooperative agreements for the acquisition of all cybersecurity related products and services by 7/1/2018.**

**Response: This recommendation has been implemented.** Cooperative agreements or cooperative language in contracts is already in use for cyber security audit and assessment services and for end point protection (antivirus). This practice will continue with future cyber security contracts.

**R.13. The county should review and update IT job classifications and salary levels to reflect the current job market by 6/30/18.**

**Response: This recommendation has been implemented.** OCIT has been conducting review and analysis of IT job classifications since the beginning of the OCIT Shared Services Pilot. Under current direction from the new CIO, OCIT is looking at smaller and more unique job functions to reassess job classifications. Any updates to IT Job Classifications is not likely to take effect before June 30, 2018.

**R.14. The county should develop a succession plan covering cybersecurity-critical positions by 6/30/18 to provide for continuity of these positions.**

**Response:** **This recommendation has been implemented.** Succession planning is centered on cyber security and privacy management job functions with similar levels of regulatory accountability.

**R.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.**

**Response:** **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 CSJTF.

**R.16.** **OCIT should draft and implement standardized procedures for mandatory use of full disk encryption and remote final/wipe capabilities for countywide mobile devices by 7/1/2018.**

**Response:** **This recommendation requires further analysis.** These are two entirely different technologies. OCIT has engaged a third party vendor and its internal OCIT Shared Services management team to select a robust disk encryption solution for OCIT and OCIT managed information systems. Mobile Device Management (MDM) is the technology that needs to be applied to mobile devices. MDM is already in place, and countywide cyber security assessments are in process.

**R.17.** **OCIT should establish standardized procedures for IT's examination and removal of sensitive information on county digital devices, prior to their removal from county premises through transfer, sale, scrap or reuse by 12/31/17.**

**Response:** **This recommendation has not yet been implemented but it will be implemented in the future.** Disposition of data is addressed in draft Data Classification guidelines and handling instructions. Final process and policy concerning this issue will be included as technical and operational control under the CSJTF Cyber Security Policy and Process Manual which is scheduled to be submitted for review by the IT Executive Council in March of 2018.

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

**Response:** **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 (Internet) 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.