



MEMORANDUM

Date: May 23, 2016

To: The Honorable Chair and Members
Pima County Board of Supervisors

From: C.H. Huckelberry
County Administrator *[Signature]*

Re: **Questions Raised by the Board of Supervisors in the May 10 and May 17, 2016 Budget Hearings**

During the May 10 and May 17, 2016 Public Hearings regarding the proposed Fiscal Year 2016/17 budget, the Board of Supervisors heard from the Treasurer and several general government services and public works departments.

As indicated when the Budget Hearings began, we are responding in writing to the questions raised to ensure clarity of budget review and understanding. This memorandum is a response related to the May 10 and May 17 Budget Hearings.

County Administrative Overhead

Several questions were asked about the components of County Administrative Overhead and which components are driving the related budget changes. In a separate communication, a schedule of County Administrative Overhead will be provided identifying the various components and showing which components are driving the change for each department.

Economic Development and Tourism

The Proposed Tentative Adopted Budget recommends \$1.5 million in payments to other agencies. My May 24, 2016 Tentative Budget Adoption memorandum explains the changes to these payments from what was preliminarily requested by the department. The specific agencies and their budgeted amounts are shown in the table below.

Economic Development and Tourism, Payments to Other Agencies.

Agency	Budgeted Amount
Ajo Chamber of Commerce	\$ 33,887
El Tour de Tucson	30,000
JobPath	500,000
Sun Corridor Inc.	651,000
Tucson Botanical Gardens	36,397

**Economic Development and Tourism,
Payments to Other Agencies.**

Agency	Budgeted Amount
Tucson Children's Museum	48,647
Tucson Pima Arts Council	110,971
Tucson Meet Yourself	27,930
DM 50 Advocacy Effort	60,000
Total	\$1,498,832

Information Technology

Please see the attached memoranda from the Information Technology Department Director regarding the County's information technology security and the department's deputy directors (Attachment 1).

Health Benefits Trust Fund

The annual administrative cost for 2013, the last year United Healthcare administered Pima County's fully insured program, was \$3.5 million for 5,227 enrolled employees. The annual administrative cost for 2016 with Aetna administering our self-insured employee healthcare program was \$2.2 million for 5,205 enrolled employees. Pima County is currently saving an estimated \$1.3 million each year in administrative healthcare costs by using Aetna for its self-insured healthcare program.

Transportation

Attachment 2 is a schedule presenting the initial, annual and lifecycle costs of maintaining a traffic signal intersection as compared to the cost of a roundabout.

CHH/mjk

Attachments

- c: John Bernal, Deputy County Administrator for Public Works
Nanette Slusser, Assistant County Administrator for Policy, Public Works
Tom Burke, Deputy County Administrator for Administration
Jan Leshar, Deputy County Administrator for Community and Health Services
Keith Dommer, Director, Finance and Risk Management
Robert Johnson, Budget Manager, Finance and Risk Management

ATTACHMENT 1

Date: May 17, 2016

To: Chuck Huckelberry
County Administrator

From: Jesse Rodriguez
Chief Information Officer

Via: Tom Burke
Deputy County Administrator for Administration

Re: ITD Security Division

At the Information Technology Department (ITD) FY 16/17 budget presentation on May 10, 2016, Supervisor Elias requested that I update the Board on what Pima County was doing to secure our information systems. The following data is intended to provide clarification concerning information security within Pima County Government. The intent of this document is to provide enough insight into the issues we are facing, the impact cyber threats are currently having on our organization, as well as what we are likely to see in the future, and some steps ITD is taking to get us where we need to be.

The issues we face today are quite complex because cyberterrorism has become such a moneymaking proposition. Cyber criminals have created immense networks of threat actors (hackers) utilizing the dark web to share tools and knowledge to create never seen attack vectors on a daily, hourly and/or by the minute basis intended to outsmart the security tools most organizations like ours can afford. These cybercrime networks have seen script kiddies (unskilled individuals that use scripts others have created to deface websites and be a general nuisance) and made very complex tools and scripts available to them at minimal cost, so they no longer use the tools to be a nuisance, but instead use them to steal data, often resulting in large ransom payments. For Pima County the data these threat actors are after include, but are not limited to, credit card data (Payment Card Industry known as PCI), Personally Identifiable Information (PII) on employees and constituents, Health data (Health Insurance Portability Accountability Act known as HIPAA), tax roll data, and voter data.

As we have witnessed in a major way over the past three months, cyberterrorists are using SPAM email and Phishing attacks as one attack vector to gain access to our employee accounts, our computing devices, and in the long term our data. By sending email messages that appear "just real enough" that an employee will click on the attachment or link contained within, an attack vector has just been created that will immediately begin mining critical data, or will plant malware that will spread itself throughout our environment while slowly leaking data back out to networks where cybercriminals gather and use that data for profit. These malware variants are extremely well written and are using versions of artificial intelligence to learn when our tools are attempting to stop them, they morph to a new variant, and then continue to attack our systems and data.

Based upon ongoing attacks we have encountered and responding to the findings within the recent Arizona Auditor General audit, Pima County ITD began implementing new systems and

Chuck Huckleberry, County Administrator

Via: Tom Burke, Deputy County Administrator for Administration

Re: ITD Security Division

May 17, 2016

Page 2 of 3

tool sets to fight this cyber battle more efficiently and effectively than we have been able to in the past. Examples of the strategies we are implementing are as follows:

- Antivirus (AV) solutions had not changed much over the years. They have been signature based and as providers find new viruses and malware, they create new signature files and send them out to be installed by end users to protect their devices. This type of AV software has ended up being a tool that stops fewer and fewer attacks, and is mostly used to clean up infections once computers are infected (very labor intensive). The new generation of AV software utilizes data science and machine learning algorithms to determine whether software should be allowed to execute and it stops the malware / viruses before they can even infect a computer. This new generation of AV software also stops infected websites from running code when compromised sites are accessed. ITD is currently running a proof of concept on a new generation product that catches 99% of all known and unknown virus / malware.
- Web filtering solutions have many more capabilities than they have in the past so we are updating our filtering system to a solution that is capable of searching much deeper into website queries to determine if staff should be allowed to access sites. It blocks attachments and links within SPAM / Phishing emails which staff members tend to click on, and which is one of our greatest vulnerabilities.
- The primary focus of the recent audit findings revolved around the County's ability to secure, access, modify and recover data. The County IT Department is developing a series of Administrative Procedures based on the National Institute of Standards and Technology ((NIST) – the standards the AZ Auditor General audits against), best practices. Within our current environment, we have large amounts of data that are very difficult to determine vulnerabilities and attacks. ITD is in the process of acquiring software that correlates all of that data from our applications, users, network, and datacenters and analyzes it within a centralized database engine to provide ITD staff with actionable data within milliseconds of an event, instead of staff spending weeks and/or months manually reviewing records to figure out what is / was going on.
- Microsoft has also taken a lead role in creating tools that help secure their operating systems, office products and end user devices. We have implemented several of their tools and continue to implements others. Tools already implemented are:
 - 1) Local Administrator Password Solution ((LAPS) – helps prevent Denial of Service attacks).
 - 2) Password security and account lockout policies.
 - 3) Critical and Security patches are now immediately installed.
 - 4) Microsoft Direct Access is being utilized to allow mobile devices to access County data securely.
 - 5) BitLocker which encrypts all of the data that is on a computer's hard drive, making it useless to criminals.

Chuck Huckleberry, County Administrator

Via: Tom Burke, Deputy County Administrator for Administration

Re: ITD Security Division

May 17, 2016

Page 3 of 3

- Microsoft security projects we still are working on are:
 - 1) Credential Guard (keeps hackers from stealing accounts to steal data).
 - 2) Windows Defender (another layer of protection against viruses and malware).
 - 3) Active Directory Digital Rights Management (ADDRM) which will keep cyber terrorists from being able to utilize our data if they are somehow able to steal it from our network.
- Pima County has joined Arizona Cyber Threat Response Alliance (ACTRA) which serves as a hub for cooperative action against cybercrimes across many different industries and law enforcement. ACTRA is also a part of the FBI's Arizona Infragard Program which is tasked with protecting our nation's infrastructure through mutual information sharing.

The goal of our security endeavors are to create multiple layers that cybercriminals will need to breach, from the perimeter of the County's network, all the way to an individual employee and even down to the application level, in order to gain access to the County's data sources.

I know this is a rather high level explanation of what the County is doing to protect our information systems and hope that this is a sufficient to allay any concerns the Board may have.

DH/mk

c: Dan Hunt, Information Security Officer

Date: May 17, 2016

To: Chuck Huckelberry
County Administrator

From: Jesse Rodriguez
Chief Information Officer

Via: Tom Burke
Deputy County Administrator for Administration

Re: Information Technology Department Executive Leadership Team

Please accept this document as response to the question from Supervisor Elias during the May 10, 2016, FY16/17 Information Technology Department (ITD) budget review regarding the number of direct reports to the Chief Information Officer (CIO). The exceptionally demanding and diverse industry of Information Technology requires an equally customized support structure. Of particular note are the various sub-disciplines of Information Technology which require diverse, and sometimes contradictory, skill sets.

In order to effectively manage ITD operations with the proper level of focus and with the proper background, education and training for each area, my direct reports are as follows:

David Fernandez, Deputy Director for Client Services, leads the group responsible for Client Computing whose skills are used daily in Help Desk, Network Operations Center, Client Services, Applications Support and Training activities. These are primarily first and second tier support services, dedicated to client-facing activities that assist in the day-to-day operation of desktop, laptop and tablet computers and the software that runs on them. Mr. Fernandez's background in Information Systems and Client Support is critical for understanding the issues faced by these teams and to understand improvements in staffing, training and operational procedures required to mitigate the impact of issues among the 8000 client computers in Pima County. Mr. Fernandez's group is also leading the County's transition to the latest Windows operating system and associated software while maintaining an on-going deployment schedule of new computers on a rotating basis every three years to each and every county employee we support.

Mark Hayes is the Deputy Director for Relationship Management. Mr. Hayes' team of Relationship Managers (RM's) establishes working interactions with each County department, including the elected officials, to understand their system requirements and provide a single point of contact for new initiatives and to act as a conduit for enterprise initiatives such as the System Lifecycle Management endeavors for both end user computing and software standardization. The Business Analysts (BA's) who support the RM's are analysts trained to develop understanding of the business processes in the departments and the systems which sustain them. These individuals possess a fairly unusual combination of comprehending both business rules and technology, making them the bridge between the business community and the rest of ITD. Using their

Chuck Huckelberry, County Administrator

Via: Tom Burke, Deputy County Administrator

Re: Information Technology Department Executive Leadership Team

May 17, 2016

Page 2 of 4

communication skills, they devise new projects and deployments to increase the capabilities of the departments to serve their various missions. Mr. Hayes's long career in IT has been primarily focused in these areas, so he is ideally qualified to lead this effort.

Anthony (Tony) Casella is the Deputy Director for Infrastructure. His subject matter experts support the county's Infrastructure needs, server operations, data storage, networking and telecommunications. These are the hardware technical experts without whom none of the software and support operations could function. Mr. Casella's career has been spent in building and maintaining operating environments such as the County's in which large scale computer hardware is deployed in a fashion which not only meets the current needs, but anticipates the growth and technical evolution in this sector which will not impede the County's future and growing needs. He was also instrumental in the development and support of the Pima County Wireless Integrated Network (PCWIN). The skills, experience and training of his team are unique to this niche of IT, and so must be the management of it.

Dan Hunt is the County's Security Officer whose team institutes policies and procedures which protect the network from intrusions, viruses, etc., and takes the lead role in auditing IT systems and applications to ensure the County is meeting the National Institute of Standards and Technology (NIST) criteria and closing all known security vulnerabilities. The importance of this is not only the risk of the data or systems being tampered with, but also the reduction of time spent resolving any issues after they occur. The function of security officer is relatively new compared to others in IT, but it requires intense focus, certification and constant study to stay ahead of rapidly evolving threats. As this is a new team for the organization, Mr. Hunt has been tasked with first identifying the vulnerabilities and proposing an IT Governance Plan to support the resolution of current audit findings, as well as further securing the organization from potential cyber threats. Security is a rapidly evolving and extremely important IT area in most major public and private organizations.

David Wieters, the Project Management Officer, oversees Records and Compliance, ITD budget and project planning and prioritization. Records and Compliance serves to qualify hardware and software purchases for the County, including for elected officials, and ensuring procedure is followed leading into the activities controlled by Procurement. A thorough knowledge of Procurement policies and procedures is required in this role. This group also monitors asset inventory of the county's computers and software to ensure we stay in proper licensing compliance. As the budget administrator for ITD, Mr. Wieters and his team manage a \$35 million budget (in FY15/16), covering all the various areas outlined in this memo. The degree of specialized knowledge and budget control expertise required for this function are absolutely essential to maintaining integrity of this process. As well, Mr. Wieters is also establishing the County's first ITD Project Management Office, with the associated tools and procedures needed to manage a portfolio of over 100 project requests from the departments, as well as internal to ITD to

Chuck Huckelberry, County Administrator

Via: Tom Burke, Deputy County Administrator

Re: Information Technology Department Executive Leadership Team

May 17, 2016

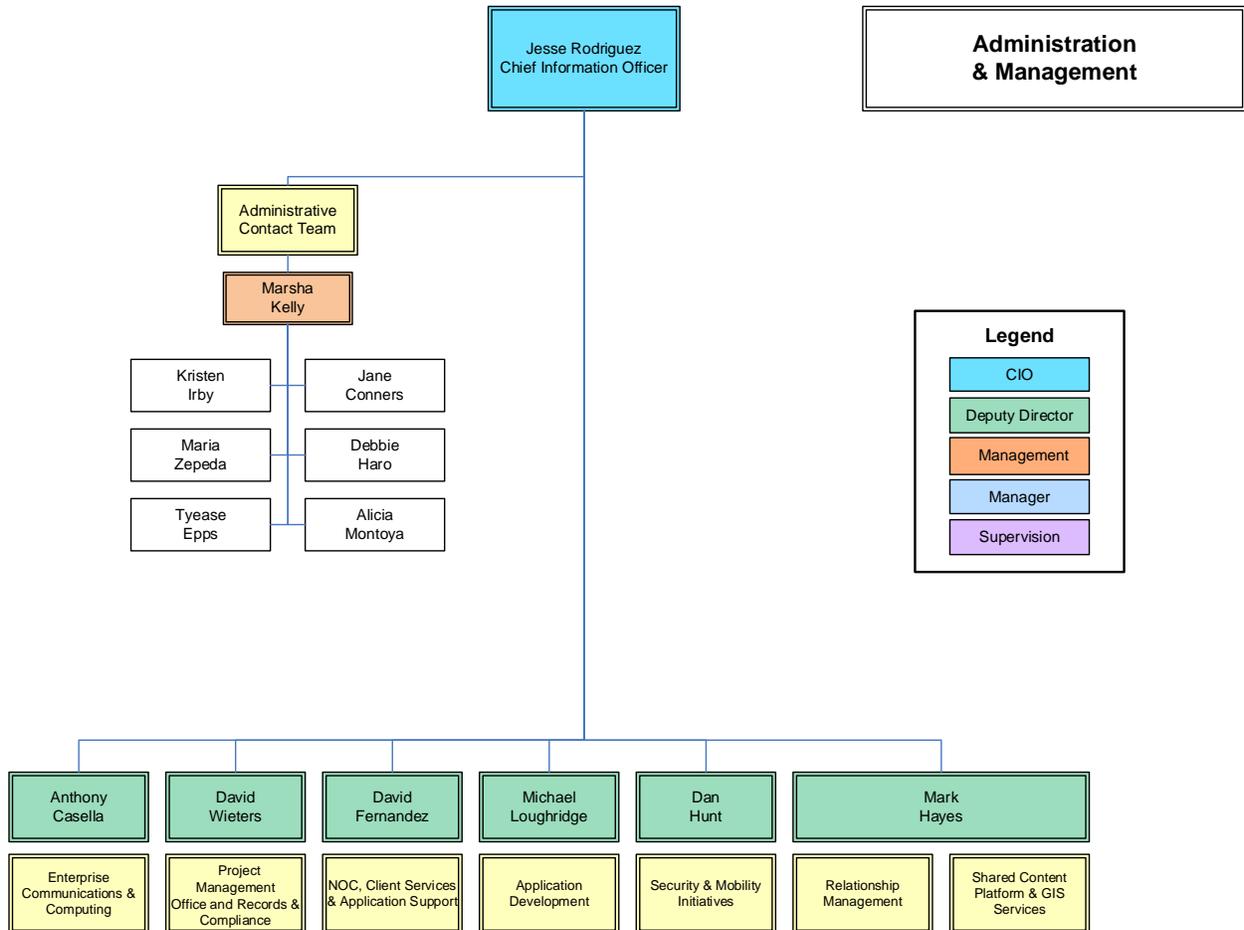
Page 3 of 4

maximize the County's resource, budget and timeline constraints to ensure that projects come in within budget and on time.

Michael Loughridge is our Applications Administrator. His group of software experts are proficient in software engineering. Mr. Loughridge's team is responsible for implementing in-house developed solutions that enhance departmental business operations, as well as implementations of the County's legacy application packages (AMS, ADP, Hansen, Maximo, etc.) A major initiative for Mr. Loughridge's team is building the Business Intelligence Framework, which will transform the way the County accesses data and turns it into actionable information. His resources are primarily software developers, trained and educated in programming languages and development techniques particular to creating computer programs. This is a skill set completely different than that of any of the other groups outlined above. Mr. Loughridge's background and talents are uniquely suited for this role.

On the following page, I have provided an organizational chart to show a visual representation of ITD's administration.

ITD Administration



Summary

Each of these individuals were selected to fill deputy level positions which are logically divided by expert area and management threshold. These positions were created to best compartmentalize, yet interrelate, specific duties for the most effective use of talent and efficient use of the workday. My direct reports were chosen for their extensive backgrounds in their knowledge areas and their proven ability to lead teams. Taken individually, they represent the best leadership for their respective functions and teams. Collectively, they are a superb unit of complementary parts which knit ITD into a whole greater than the sum of its parts for the betterment of the County.

JR/mk

ATTACHMENT 2

Cost Estimate Comparisons of a Traffic Signal vs a Roundabout

#	Description	Traffic Signal	Roundabout	Comparison
1	Initial Capital Costs	\$560K	\$600K	A Roundabout costs \$40K (7%) more to construct than a Traffic Signal intersection
2	Annual Operating and Maintenance Costs	\$13K	\$2K	A Traffic Signal costs \$11K (85%) more per year to operate and maintain than a Roundabout
3	Annual Indirect Costs (Safety, Capacity, and Liability)	\$178K	\$102K	A Traffic Signal costs \$76K (43%) more per year for non-maintenance costs to Pima County
4	Total Annual Costs (Total of Rows 2 and 3)	\$191K	\$104K	A Traffic Signal costs \$87K (46%) more per year for combined maintenance and non-maintenance
5	Total 30-year Life Cycle Cost (Row 4 times 30, plus Row 1)	\$6,290K	\$3,720K	A Roundabout saves \$2,570K (41%) over 30 years, compared to a Traffic Signal intersection

Item #	Item Name	Definition
1	Initial Capital Cost	<p>The total materials, labor, and vehicle costs to plan, design, construct, inspect, test, and administer the project from inception to final acceptance. Sometimes, right-of-way and land acquisition, as well as drainage issues must be addressed and resolved as part of a traffic control capital improvement project.</p> <p>This is a one time expense at the beginning of the improvement project's life span. Unfortunately, it is often the primary consideration in the decision process.</p>
2	Annual Direct Operating and Maintenance Costs	<p>This is the direct cost per year to perform maintenance on the electrical and mechanical equipment at the intersection. This includes routine preventive maintenance and troubleshooting, as well as observations, adjustments, and repairs in response to citizen calls. Also, questions and concerns related to operations and signal timing, damage repairs related to vehicle crashes and storms, and scheduled replacement of lights, batteries, and other equipment items with a limited useful life span fall into this category. Finally, this category includes paying the monthly electric bill for the intersection, tracking the warehouse and field inventories, and monitoring the operational status of the equipment. Over the entire lifetime of the improvement, typically 30 years, the operating and maintenance costs can far exceed the initial capital cost.</p>
3	Annual Indirect Costs (Safety, Capacity, and Liability)	<p>This category contains estimated costs due to crashes, delays, and law suits filed against the County. These costs are not as obvious as direct O & M costs, but can be significant in the long term. As with operating and maintenance costs, these "hidden" costs can far exceed the initial capital cost.</p>
4	Total Annual Costs	<p>This is simply the sum of the direct and indirect categories of yearly costs indicated above.</p>
5	Total 30-year Life Cycle Cost	<p>This bottom-line figure is calculated by multiplying the total annual cost by the anticipated 30-year life span of the improvement, then adding the one-time initial capital cost. As is normally the case for traffic control projects, the annual costs over 30 years far exceeds the initial capital cost. In the case of a traffic signal versus a roundabout, the larger initial cost of the roundabout is far outweighed by its lower Annual O & M and Indirect Costs.</p>

