

Information Technology

Paul LaValley – Chief Information Officer

101-1900	FY 20/21 Adopted Budget	FY 21/22 CAO Recommended	Change
EXPENDITURES			
Salaries and Benefits	\$2,329,903	\$2,369,725	\$39,822
Services and Supplies	\$1,523,939	\$1,856,902	\$332,963
Other Charges	(\$2,756,620)	(\$2,733,548)	\$23,072
Fixed Assets			\$0
TOTAL EXPENDITURES	\$1,097,222	\$1,493,079	\$395,857
REVENUE			
Fed/State			\$0
Grant			\$0
Realignment			\$0
Fees/Misc	\$446,119	\$144,254	(\$301,865)
TOTAL REVENUE	\$446,119	\$144,254	(\$301,865)
FUND BALANCE	\$0		\$0
NET COUNTY COST	\$651,103	\$1,348,825	\$697,722

Program Description

The Information Technology Department continually works to fulfill its mission to provide highly available, innovative, secure, cost-effective, and compliant services for Yuba County and related agencies, by partnering with business leaders, implementing appropriate technology and enabling best practices for all government functions.

The Information Technology Department needs to help the County plan for the future. There are multiple trends that will support the future vision of electronic government.

1. Cloud-based services
2. Mobility
3. Using the web to better access information and communicate
4. Integrating more collaboration tools for remote workers

While supporting programs to move the county toward these trends, we need to make sure we are compliant with increasingly strict security requirements. We must minimize the county's exposure to cyber security risks, while balancing the needs of a remote workforce.

We also need to plan to migrate off expensive and difficult-to-maintain legacy platforms, and move all departments to more efficient business processes for core public administration and public safety functions.

Information Technology

Paul LaValley – Chief Information Officer

Even with the ongoing changes in technology, we continually look to decrease costs for equipment and services used across the county. We always seek other ways to minimize our cost structure and still meet required levels of service.

Accomplishments

FY 2020-2021

The Information Technology Department completed several projects that improved overall availability and security, as well as provide new capabilities. Some of the significant projects include:

1. Deployed 500+ additional mobile computers for teleworkers
2. Increased Internet connection speed more than 3-fold to 1Gbps (Giga bits per second)
3. Implemented new VPN infrastructure to fully support Multi-factor Authentication, as required by DOJ and IRS
4. E-fax
5. Installed 10 Gig Microwave Links to Government Center, Courthouse, Packard, Animal Care, and Public Works Airport facilities
6. Managed the planning and completion of Sheriff Dispatch Radio Console Replacement

Performance Measures

FY 2020-2021

The ultimate purpose for Information Technology in any organization is to increase the efficiency and effectiveness of business operations. Achieving this purpose requires both the implementation of technology and users who are trained and motivated to use it. This ultimately means that many goals must be shared between IT and customer departments, as described below.

For metrics on processes the IT department more fully controls, we will use the following.

1. Availability for key services
2. Security (critical security incidents)
3. IT spending Metrics (Benchmarked against Gartner Local Government with less than \$250 budget)
 - a. IT Spending as a Percent of Operating Expense
 - b. IT Spending per Employee
4. IT Full-Time Equivalent as a Percent of Employees

Goals and Objectives

FY 2021-2022

1. Work with the Office of Emergency Services and departments to document business continuity plans, including systems and networks used with contingency plans

Information Technology

Paul LaValley – Chief Information Officer

2. Document all older systems that are no longer supportable or securable
3. Communicate older systems status to departments and work on migration plans
4. Deploy updated EDR (Endpoint Detection and Response) systems (Windows Defender for Endpoint or Sophos) to all computers
5. Improve endpoint patching process and vulnerability assessment and remediation
6. Harden Active Directory (AD) infrastructure, to the extent possible
7. Start countywide user security awareness training and phish testing program
8. Deploy Darktrace Immune System platform for neutralizing advanced ransomware in real time using the platform's Autonomous Response technology, which will contain malicious activity in seconds, surgically neutralizing attacks while letting normal business operations continue. The technology intelligently adapts to threats as they unfold and provides 24/7 coverage of the entire workforce, when security teams are overwhelmed or simply aren't around.

Pending Issues/Policy Considerations FY 2021-2022

The amount of telework required as part of the COVID pandemic response and the ransomware event in February of 2021 reminded us of several things:

1. The county is highly dependent on information technology to complete its mission
2. The IT department is not adequately staffed to quickly respond to significant changes or issues
3. Due to the sophistication of cyber attackers and escalating attacks, we need a more active cyber defense posture
4. We need to migrate older infrastructure to modern, secure, supportable platforms

The pandemic forced IT to deploy 100's of extra computers for departments that moved to primarily telework. We also had to upgrade our internet connection and VPN infrastructure, to support large-scale, long-term remote work. We also implemented some systems (e-fax) to move paper documents to electronic form (emails).

The IT department has been surviving with just enough personnel to handle existing workload but has not been able to effectively deal quickly enough with any significant changes. This was demonstrated by

Information Technology

Paul LaValley – Chief Information Officer

the initial pandemic response, the ransomware incident and the recent loss of an employee to a private sector opportunity. To exacerbate the personnel issue, all but 4 of the department's current 15 employees are eligible to retire. The department needs to add people to be able to better support county plans – primarily organization excellence strategic priorities. We also need to make sure that we have succession plans in place, as well as development plans to bring in new people into the department and grow them into roles of more responsibility. Expanded IT headcount will help the department support future county plans.

The ransomware attack was a very painful educational experience. It exposed the county to international, financial, cyber-terrorism using tools and techniques that we did not previously know existed. The ransomware attack and the increasing number of cyber-attacks (for example, the SolarWinds attack of late 2020 and the Microsoft Exchange attack of late 2021) makes it clear that cyber defense needs to be a major focus for all organizations (public and private sector) moving forward. Ultimately, this means more internal resources are needed in IT organizations, and more expertise is needed from vendors and service providers.