

**COUNTY OF MADERA
BUDGET UNIT DETAIL
BUDGET FOR THE FISCAL YEAR 2022-23**

Department: Information Technology
Security (00243)
Function: General
Activity: Other General
Fund: General

	BOARD APPROVED <u>2020-21</u>	BOARD APPROVED <u>2021-22</u>	DEPARTMENT REQUEST <u>2022-23</u>	CAO RECOMMENDED <u>2022-23</u>
<u>ESTIMATED REVENUES:</u>				
CHARGES FOR CURRENT SERVICES				
662800 Interfund Revenue	0	14,692	49,623	49,623
662802 Interfd Rev - Comp Svc	4,123			
TOTAL CHARGES FOR CURRENT SERVICES	4,123	14,692	49,623	49,623
MISCELLANEOUS REVENUE				
670000 Intrafund Revenue	1,422,142	1,796,407	2,078,647	2,078,647
TOTAL MISCELLANEOUS REVENUE	1,422,142	1,796,407	2,078,647	2,078,647
OTHER FINANCING SOURCES				
680200 Operating Transfers Out	10,862	0	0	0
TOTAL OTHER FINANCING SOURCES	10,862	0	0	0
<u>TOTAL ESTIMATED REVENUES</u>	<u>1,437,127</u>	<u>1,811,099</u>	<u>2,128,270</u>	<u>2,128,270</u>
<u>EXPENDITURES:</u>				
SALARIES & EMPLOYEE BENEFITS				
710102 Permanent Salaries	322,661	332,199	352,444	352,444
710105 Overtime	2,941	2,500	3,000	3,000
710106 Stand-By	13,386	20,000	20,000	20,000
710200 Retirement	124,068	131,052	143,127	143,127
710300 Health Insurance	39,089	45,965	47,916	47,916
TOTAL SALARIES & EMPLOYEE BENEFITS	502,146	531,716	566,487	566,487
SERVICES & SUPPLIES				
720300 Communications	3,245	4,000	4,000	4,000
720800 Maintenance - Equipment	24,420	131,000	89,500	89,500
721200 Miscellaneous Expense	12,291	12,291	14,000	14,000
721300 Office Expense	12,017	14,400	14,400	14,400
721400 Professional & Specialized Services	170,798	208,300	329,300	329,300

**COUNTY OF MADERA
BUDGET UNIT DETAIL
BUDGET FOR THE FISCAL YEAR 2022-23**

Department: Information Technology
Security (00243)
Function: General
Activity: Other General
Fund: General

	BOARD APPROVED <u>2020-21</u>	BOARD APPROVED <u>2021-22</u>	DEPARTMENT REQUEST <u>2022-23</u>	CAO RECOMMENDED <u>2022-23</u>
SERVICES & SUPPLIES(continued)				
721426 Software	441,523	646,887	921,342	921,342
721900 Property Tax	2,150	8,151	10,000	10,000
722000 Transportation & Travel	6,677	22,480	49,700	49,700
TOTAL SERVICES & SUPPLIES	673,121	1,047,509	1,432,242	1,432,242
OTHER CHARGES				
730302 Retire Capital Assets	450,278	450,278	415,740	415,740
TOTAL OTHER CHARGES	450,278	450,278	415,740	415,740
FIXED ASSETS				
740300 Equipment	0	0	35,000	35,000
TOTAL FIXED ASSETS	0	0	35,000	35,000
<u>TOTAL EXPENDITURES</u>	<u>1,625,545</u>	<u>2,029,503</u>	<u>2,449,469</u>	<u>2,449,469</u>
<u>NET COUNTY COST (EXP - REV)</u>	<u>188,418</u>	<u>218,404</u>	<u>321,199</u>	<u>321,199</u>

INFORMATION TECHNOLOGY – INFORMATION SECURITY

COMMENTS

In alignment with the organizational strategic plan “Mission 2023”, the Office of Information Technology (OoIT) will push forward with the continued implementation (year 4 of 5) of the Information Security Strategy. Over the first three years of Mission 2023, OoIT has significantly improved the organizations compliance and security posture. Increased posture derives from the ongoing optimization of tools. Therefore, tool and process optimization is a primary focus of Fiscal Year 2022-2023. Additionally, as adversaries evolve, compliance tightens, and insurance requirements increase, so does the need to deploy new technology and processes. In Fiscal Year 2022-2023, the OoIT will continue to layer our security to protect against new threats and shrink gaps in protection shortcomings. Moreover, a higher focus on the human element will be addressed through increased phishing simulation and security awareness training. The objectives of the information security program are to safeguard confidentiality of information, upkeep the integrity of data, and increase the availability of systems and operations. Leveraging compliance and insurance requirements as a guide, the information security program will improve the security of Federal Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), Criminal Justice Information Services (CJIS), Federal Tax Information (FTI – Publication 1075), and other privacy mandates to increase the confidentiality, integrity, and availability of the County’s networks, systems, and data.

The following chart represents Madera County Departments that have been identified as receiving and/or exchanging Federal information.

Sheriff's Department	Department of Justice
Department of Corrections	Department of Justice
Probation	Department of Justice
District Attorney	Department of Justice, Department of Treasury
Child Support Services	Department of Treasury, Social Security Administration
Department of Social Services	Department of Treasury, Social Security Administration, Department of Justice
Public Health	Social Security Administration and Women, Infants and Children
Behavioral Health Services	Social Security Administration

Cyber threats and criminal activity are prevalent in today’s world and public sector agencies are not immune from these exploits. The Verizon 2021 Data Breach Investigations Report has the following comments of Public Administration: “by far the biggest threat in this industry is the social engineer. Actors who can craft a credible phishing email are absconding with Credentials at an alarming rate in this sector”. In addition, Verizon states in the public sector 96% of breaches were financially motivated (up 10% from 2020), and 92% of public administration breaches were the result of Social Engineering and System Intrusion (adversary unauthorized software installation via malware). According to Forbes, as of October 2021 the Identity Theft Resource Center (ITRC) declared the number of publicly reported breaches has already exceeded the total for 2020. This is a single year record. These statistics are concerning, and with a 17.5% increase

INFORMATION TECHNOLOGY – INFORMATION SECURITY

to the County's threat surface (300 additional devices) since 2019, an increase in focused resources and energy to protect County resources will be necessary.

To combat the continued increase in nefarious cyber activity OoIT has developed a strategy to evolve a team with a mixture of on staff engineers/analysts/technicians and highly specialized outsourced professionals. In addition, to address the ever-growing social engineering challenge, the County will focus on real-world phishing simulations and phishing specific training. Moving towards compliance with the NIST Cybersecurity Framework and various regulatory mandates will not ensure complete protection from cyber threats. However, moving closer to compliance will assist the County in developing a proactive approach to the prevention of nefarious cyber activity from internal and external threats. In addition to cyber threat prevention, striving for NIST compliance will allow the County to better prepare should it become a victim of an internal or external information breach or cyber-attack.

WORKLOAD

Key components of the Information Security budget include:

- Development, upkeep, and success measurement of Information Security Program, including but not limited to: security governance, strategy, policies, standards, control implementation, contract hardening, etc.
- Threat, Vulnerability, Impact Assessment, and Patch Management
- Backup management – policy, retention development, auditing (report monitoring), validate recovery testing
- Inventory and System Development Life Cycle (SDLC)
- Network Monitoring Operations & Security Monitoring Operations
- Incident Management
- Security Awareness Training
- Data room physical security and data protection
- Network threat detection and defense system management
- Security architecture, design, and control implementation
- Business Impact Analysis (BIA) and Risk Assessment

Planned activities:

- Security strategy and year 4 of 5 roadmap implementation
- Phishing Simulation and end-user training

INFORMATION TECHNOLOGY – INFORMATION SECURITY

WORKLOAD (continued)

- Backup data protection from ransomware
- Credential protection through Multi-Factor Authentication optimization
- Revised Security Operations Center (SOC) and Audit Log Collection
- Certificate monitoring and maintenance
- Browser Plug-In discover, revocation, and monitoring
- Lessened threat surface through vulnerability identification and patch management
- Mobile workforce onboarding and organizational requirements implementation
- Continued optimization of network visibility tools
- Backup process improvement and architecture expansion and maintenance
- Network segmentation and zero-trust network expansion
- Internal & External network penetration testing and vulnerability assessment
- Incident Response partnership, business process design, and incident exercises
- Computer room enhancement and physical security improvement
- Expanded Security Awareness training as required by compliance agencies (e.g. FTI, FSMA, CJIS, HIPAA, etc.)
- Revision of Network Security Policy to align with NIST 800-53 Revision 5 (Draft)
- Maintenance and support for perimeter and internal firewall connections
- Maintenance and support for security appliances (SPAM, Web filters, IPS/IDS, Advanced Malware Protection)
- Maintenance and support for anti-virus and advanced malware systems
- Maintain backup process and offsite media (tapes) management for data restoration
- Offsite cloud storage for backup data review, planning, and pilot
- Remote access and vendor support management
- Security licensing for current level threat surface and current number of end points including known computers, laptops, cell phones, printers, IOT devices, etc.
- Secure additional devices – Due to the addition of approximately 300 devices added to the network in FY 2020-21, the County's threat surface has increased by approximately 17.5%

INFORMATION TECHNOLOGY – INFORMATION SECURITY

ESTIMATED REVENUES

- 662802** **Interfund Revenue** (\$49,623) is recommended increased \$34,931 for charges to other departments for Network Information Security Services.
- 670000** **Intrafund Revenue** (\$2,078,647) is recommended increased \$282,240 for charges to other departments for Network Information Security Services.

SALARIES & EMPLOYEE BENEFITS

- 710102** **Permanent Salaries** (\$352,444) are recommended increased \$ 20,245 to fund the security positions.
- 710105** **Overtime** (\$3,000) is recommended increased \$500 to fund expected overtime related to cyber security incidents or projects.
- 710106** **Stand-By** (\$20,000) is recommended unchanged to fund Stand-By pay for network security staff. Due to increasing cyber threats after hours, on weekends, and holidays, it is necessary to have network security staff available for immediate response if necessary.
- 710200** **Retirement** (\$143,127) is recommended increased \$12,075 to fund Retirement costs.
- 710300** **Health Insurance** (\$47,916) is recommended increased \$1,951 to fund Health Insurance costs.

SERVICES & SUPPLIES

- 720300** **Communications** (\$4,000) is recommended unchanged to fund the following:
\$4,000 Cell Phone Service
- 720800** **Maintenance – Equipment** (\$89,500) is recommended decreased \$41,500 to fund the following:

INFORMATION TECHNOLOGY – INFORMATION SECURITY

720800 **Maintenance – Equipment (continued)**

Maintenance – Recurring Costs

\$35,000	Backup Expansion (yearly growth)
\$42,000	CISCO Smart Net
\$2,500	San Switch Maintenance
\$10,000	Overland Maintenance

721200 **Miscellaneous Expense** (\$14,000) is recommended increased \$1,709 to fund the following:

\$14,000	ConvergeONE Lease – Sales Tax on Capital Lease
----------	--

721300 **Office Expense** (\$14,400) is recommended unchanged to fund the following:

\$6,000	Back Up Tapes
\$1,000	Office Supplies
\$ 7,400	Computer Equipment

721400 **Professional & Specialized Services** (\$329,300) is recommended increased \$121,000 to fund the following:

Professional Services – Recurring Costs

\$ 5,000	Hard Drive Destruction
\$ 16,000	External Consulting Services and Support
\$ 800	ISACA Memberships
\$ 68,000	Cisco Talos Incident Response
\$ 28,000	Trace Digital Forensics Services
\$ 5,000	Insight Synology
\$ 65,000	Cloud Back Up – New

Professional Services – New Recurring Costs

\$ 19,500	Ransomware Protection
\$ 82,000	Business Continuity Planning - Network & Security Perspective
\$ 40,000	Internal Penetration Assessment

INFORMATION TECHNOLOGY – INFORMATION SECURITY

721426 **Software** (\$921,342) is recommended increased \$274,456 to fund the following:

Software – Licenses, Support, and Subscription Services – Recurring Costs

\$12,096	Endpoint Detection and Response (EDR) Software– Annual Subscription License – 750 Licenses (Prepaid Expense Year 4 of 4 @ \$12,096/year)
\$ 20,000	Secure File Transfer Solution
\$ 54,000	Enterprise Backup Software – Annual License and Maintenance
\$ 5,000	Enterprise Backup Data DeDuplication Software
\$12,000	Manage Engine Active Directory Audit Plus
\$ 5,800	Active Directory Manager
\$ 25,000	Multi Factor Authentication Tokens
\$18,000	Snapshot Configurations
\$ 3,500	Password Management Vault
\$ 50,000	Network Operations Center (NOC) Server Infrastructure Health Monitoring – Annual Subscription
\$ 45,000	Security Awareness Training – Annual Subscription
\$ 10,600	SSL Certificates
\$ 49,000	Vendor Secure Remote Access – Annual Subscription
\$ 7,784	Private Cloud Licenses for Virtualization Infrastructure (Prepaid Expense-Year 5 of 5 @ \$7,784/year)
\$ 15,000	Network Infrastructure Monitoring, Mapping, and Backup – Annual License and Maintenance
\$ 6,200	Penetration/Vulnerability/White Hat Training – Software Subscription
\$ 7,700	Management Security Training – Software Subscription
\$ 70,000	External Penetration Analysis and Vulnerability Scanning – annual subscription
\$ 16,000	Mobile Device Management Software – Annual Maintenance
\$ 20,000	Integrated Electronics - Badge Software Annual Maintenance
\$ 29,540	Remote Access Mobile Device Management Licenses – 750 Devices, \$38/Device
\$ 11,122	Remote Access Mobile Device Management User License Maintenance (150 Licenses; \$65/User) – Annual License
\$ 4,000	Microsoft 365 Monitoring, Logging, and reporting
\$ 65,000	Security Operations Center 24 Hour Monitoring – Annual Subscription
\$ 3,500	Certificate Tracking and Management
\$ 17,000	Browser Security
\$ 2,000	Deploy and Inventory Management
\$ 15,000	Manage Engine Desktop Central and Patch Manager
\$ 20,000	Device Logging

INFORMATION TECHNOLOGY – INFORMATION SECURITY

721426 Software (continued)

Software – Licenses, Support, and Subscription Services – Recurring Costs (continued)

\$ 11,500 Training Subscription Services
\$ 290,000 System Logging

721900 Property Tax (\$10,000) is recommended increased \$1,849 to fund the Property Taxes associated with the Network and Security Project Lease

722002 Transportation & Travel (\$49,700) is recommended increased \$27,220 to fund training needs throughout the year.

\$ 49,500 Security Training Program
\$ 200 MISAC

OTHER CHARGES

730302 Rent (\$415,740) is recommended decreased \$34,538 to fund the following capital lease:

\$415,740 ConvergeOne Financial – Network Security Implementation Project (Final Payment - September 2028)

FIXED ASSETS

740301 Equipment (\$35,000) is recommended increased \$ 35,000 to fund the following:

\$ 35,000 Enterprise Back up Storage Increase - Hardware

**COUNTY OF MADERA
 BUDGET UNIT POSITION SUMMARY
 BUDGET FOR THE FISCAL YEAR 2022-23**

Department: Information Security
 00243
 Function: General
 Activity: Other General
 Fund: General

<u>JCN</u>	<u>CLASSIFICATION</u>	<u>2021-22 Authorized Positions</u>		<u>2022-23 Proposed Positions</u>		<u>Y-O-Y Changes in Positions</u>		<u>Notes</u>
		<u>Funded</u>	<u>Unfunded</u>	<u>Funded</u>	<u>Unfunded</u>	<u>Funded</u>	<u>Unfunded</u>	
3387	Network Security Engineer I or	1.0	-	1.0	-	-	-	
3388	Network Security Engineer II							
4121	Deputy CIO - Network & Security Services	1.0	-	1.0	-	-	-	
3387	Network Security Engineer I or							
3388	Network Security Engineer II or							
3389	Senior Network Security Engineer	1.0	-	1.0	-	-	-	
4222	Executive Assistant to the Dept Head	1.0	-	1.0	-	-	-	
TOTAL		4.0	-	4.0	-	-	-	

NOTES: