COUNTY OF MADERA
BUDGET UNIT DETAIL
BUDGET FOR THE FISCAL YEAR 2023-24

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

	ACTUAL 2021-22	BOARD APPROVED 2022-23	DEPARTMENT REQUEST 2023-24	CAO RECOMMENDED 2023-24
ESTIMATED REVENUES:				
CHARGES FOR CURRENT SERVICES				
662800 Interfund Revenue	0	49,623	49,623	49,623
662802 Interfd Rev - Comp Svc	16,538	0	0	0
TOTAL CHARGES FOR CURRENT SERVICES	**16,538**	**49,623**	**49,623**	**49,623**
MISCELLANEOUS REVENUE				
670000 Intrafund Revenue	1,312,280	2,078,647	2,698,966	2,698,966
TOTAL MISCELLANEOUS REVENUE	**1,312,280**	**2,078,647**	**2,698,966**	**2,698,966**
OTHER FINANCING SOURCES				
680200 Operating Transfers Out	3,272	0	0	0
TOTAL OTHER FINANCING SOURCES	**3,272**	**0**	**0**	**0**
TOTAL ESTIMATED REVENUES	**1,332,090**	**2,128,270**	**2,748,589**	**2,748,589**
EXPENDITURES:				
SALARIES & EMPLOYEE BENEFITS				
710102 Permanent Salaries	336,709	352,444	595,898	595,898
710105 Overtime	4,172	3,000	3,000	3,000
710106 Stand-By	18,916	20,000	26,624	26,624
710200 Retirement	131,920	143,127	241,994	241,994
710300 Health Insurance	41,695	47,916	121,710	121,710
TOTAL SALARIES & EMPLOYEE BENEFITS	**533,412**	**566,487**	**989,226**	**989,226**
SERVICES & SUPPLIES				
720300 Communications	3,929	4,000	4,500	4,500
720800 Maintenance - Equipment	13,475	89,500	77,500	77,500
721200 Miscellaneous Expense	4,096	14,000	0	0
721300 Office Expense	6,590	14,400	35,000	35,000
721400 Professional & Specialized Services	62,509	329,300	651,395	651,395
721426 Software	362,966	921,342	815,995	815,995

COUNTY OF MADERA
BUDGET UNIT DETAIL
BUDGET FOR THE FISCAL YEAR 2023-24

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

	ACTUAL 2021-22	BOARD APPROVED 2022-23	DEPARTMENT REQUEST 2023-24	CAO RECOMMENDED 2023-24
SERVICES & SUPPLIES (continued)				
721900 Property Tax	14,373	10,000	18,000	18,000
722000 Transportation & Travel	9,198	49,700	37,380	37,380
TOTAL SERVICES & SUPPLIES	**477,135**	**1,432,242**	**1,639,770**	**1,639,770**
OTHER CHARGES				
730302 Retire Capital Assets	424,375	415,740	415,740	415,740
TOTAL OTHER CHARGES	**424,375**	**415,740**	**415,740**	**415,740**
FIXED ASSETS				
740300 Equipment	30,347	35,000	145,000	145,000
TOTAL FIXED ASSETS	**30,347**	**35,000**	**145,000**	**145,000**
TOTAL EXPENDITURES	**1,465,269**	**2,449,469**	**3,189,736**	**3,189,736**
NET COUNTY COST (EXP - REV)	**133,180**	**321,199**	**441,147**	**441,147**

COMMENTS

In alignment with the organizational strategic plan “Mission 2023”, the Office of Information Technology (OoIT) will push forward with the continued implementation (year 5 of 5) of the Information Security Strategy. Over the first four years of Mission 2023, OoIT has significantly improved the organizations compliance and security posture. Increased posture derives from the ongoing optimization of tools. Therefore, ongoing tool and process optimization is a primary focus of Fiscal Year 2023-2024. Additionally, as adversaries evolve, compliance tightens, and insurance requirements increase, so does the need to deploy new technology and processes. In Fiscal Year 2023-2024, the OoIT will continue to layer our security to protect against new threats and shrink gaps in protection shortcomings. Moreover, continued focus on the human element will be addressed through increased phishing simulation and security awareness training. It is also our intention to reduce risk by securing authentication methods and remediating internal vulnerabilities. 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

Public sector agencies are an increased target for cyber criminals and the County of Madera is not immune from these exploits. The “Verizon 2022 Data Breach Investigations Report” (DBIR) has the following comments of Public Administration: “System Intrusion pattern has drop-kicked the Social Engineering pattern right out”. This should be concerning to public agencies as system intrusion attacks are far more complex. System intrusion include Advanced Persistent Threats (APT), and APT's are typically carried out by skilled and determined adversarial groups over an extended amount of time. APT’s encapsulate an array of attack strategies including, but are not limited to: Social

Engineering, malware implants, privilege escalation, data exfiltration, denial-of-service (e.g. Ransomware), etc. To defend, public agencies will need to increase their defense strategies but most importantly their staffing and partnerships.

The Verizon DBIR states the following as motives for public sector targeting: Financial (80%), Espionage (18%), Ideology (1%), Grudge (1%). According to the "State of Cybersecurity 2021" report by ISACA, 32% of public sector respondents reported an increase in breaches in 2020, and 63% reported an increase in cyber-attacks compared to the previous year. Moreover, according to the "Global Risks Report 2021" by the World Economic Forum (WEF), the number of cyber-attacks have increased nearly six-fold over the past decade. Although numbers are yet to be released for 2022, there is strong evidence to suggest this rate of increased cybercrime will continue. These statistics are concerning, and with a 21.5% increase to the County's threat surface (320 additional devices) since 2019, and zero cybersecurity staff increase to counter act growth, defense against ATP is becoming ever more difficult. An increase in focused resources and energy to protect County resources will be necessary to decrease risk.

To combat the continued increase system intrusion attempts and advanced persistent threats, OoIT has developed a strategy to evolve a team with a mixture of on staff engineers/analysts/technicians and highly specialized outsourced professionals. To be successful, it is highly recommended additional staffing and/or external partnerships dedicated to cybersecurity is increased. 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
- Identity and Access 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
- Threat Intelligence - Network threat detection and defense system management
- Security architecture, design, and control implementation
- Risk Assessment
- Technical Contract and Statement of Work Analysis

Security Division Accomplishments 2022-23

- **Backup Process Improvement and Architecture Expansion and Maintenance:** Our team has accomplished a complete overhaul of the backup jobs, reporting, and modernized the overall infrastructure. As a result, we have achieved a number of successful outcomes. First and foremost, we have improved OoIT cross-functional transparency, enabling us to identify and address failures more quickly. In addition, we have achieved a 100% job service level agreement (SLA), which has greatly improved our overall resilience and disaster recovery capabilities. To further these capabilities, OoIT has established a secondary site for backup data. Prior to this initiative, the possibility of backup data replication did not exist. Furthermore, we have reduced the number of backup schedules by 85%, which has streamlined our operations and reduced complexity.

- **Credential Protection through Multi-Factor Authentication Optimization:** The Office of Information Technology Security Division has made significant progress in strengthening our security posture through the advancement of multi-factor authentication (MFA). Our team has achieved several key successes, including the successful launch of alpha, beta, and pilot programs, paving the way for a further rollout.

- **Decrease Threat Surface Through Vulnerability Identification and Patch Management:** OoIT has accomplished notable advancements in patch management and remediation. Our team has worked diligently to implement a robust patch management process, which has resulted in significant improvements to our cyber exposure. Specifically, we have improved our score by 29% in the calendar year of 2022, demonstrating our commitment to staying ahead of the latest security threats. Furthermore, our overall score is now 7% better than other public administration agencies, a clear indication of our focus on security and our dedication to protecting our IT environment.

- **Continued Optimization of Network Visibility Tools:** Our team has made significant progress in enhancing our security posture through the optimization of network monitoring tools. By improving visibility into our IT environment, we can now detect critical threats such as ransomware, internal unauthorized movement, unauthorized network scanning, fileless malware, abnormal network traffic,

foreign traffic destinations (e.g. China, Russia, etc.), unauthorized script execution, data hoarding, and malware propagation. This achievement significantly improves the security posture of our organization in several ways. First, it allows us to identify and respond quickly to potential security incidents, minimizing the impact of attacks and reducing the risk of data loss or service disruptions. Additionally, this enables us to proactively address vulnerabilities and mitigate risk.

- **Phishing Simulation and End-User Security Awareness Training:** OoIT has enhanced our security awareness program through the implementation of phishing simulations and end-user security awareness training. Our team has worked to equip our workforce with the knowledge and skills necessary to identify security threats. A pilot of phishing simulations has taken place and OoIT is prepared to increase the program by baselining our phishing click-rate. We have also given our users the ability to submit potential phishing emails to a sandbox for inspection.

- **Development and Implementation of a Technology Contract Review Process**: Madera County has successfully implemented a technology contract review process, resulting in a significant reduction of legal and financial risks associated with technology procurement. This initiative has been an important step towards ensuring that our organization's technological investments align with our strategic goals, and that we are effectively managing the risks associated with technology contracts. The implementation of the technology contract review process involved developing a cross-functional team consisting of representatives from legal and information security. This team then partners with members of IT engineers and analysts along with county department representatives. A comprehensive contract review process was created to ensure compliance with legal and regulatory requirements, identification of potential risks and liabilities, and alignment with our overall business goals. Extensive training sessions with county staff was conducted to ensure they understood the relevance. Standardized contract templates, checklists, and guides were published to the County website for future retrieval.

Anticipated Projects 2023-2024

- Continued implementation of Backup Improvement Strategy
- Increased Multi-Factor Authentication
- Vulnerability Remediation
- M365 Backup Implementation
- Increased monitoring and alerting
- Increased phishing simulation
- Malicious code monitoring and inspection
- Mobile threat defense

ESTIMATED REVENUES

662802 **Interfund Revenue** ($49,623) is recommended unchanged for charges to other departments for Network Information Security Services.

670000 **Intrafund Revenue** ($2,698,966) is recommended increased $ 620,319 for charges to other departments for Network Information Security Services.

SALARIES & EMPLOYEE BENEFITS

710102 **Permanent Salaries** ($595,898) are recommended increased $243,454 to fund the current and new security positions.

710105 **Overtime** ($3,000) is recommended unchanged $0 to fund expected overtime related to cyber security incidents or projects.

710106 **Stand-By** ($26,624) is recommended increased $6,624 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** ($241,994) is recommended increased $98,867 to fund Retirement costs.

710300 **Health Insurance** ($121,710) is recommended increased $73,794 to fund Health Insurance costs.

The Fiscal Year 2023-2024 Budget Request for Information Technology Security, ORG Key 00243, includes a request for four additional Network Security Engineers to meet regulatory requirements in the areas of Patch Management, Vulnerability Remediation, Control Testing and Audit, and Mobile Device Management. The additional cost to fund all four positions is $371,037, funded through an increase in subvented department Intrafund Revenue.

SERVICES & SUPPLIES

720300 **Communications** ($4,500) is recommended increased $500 to fund the following:

$4,500 Cell Phone Service

720800 **Maintenance – Equipment** ($77,500) is recommended decreased $12,000 to fund the following:

Maintenance – Recurring Costs

$ 45,000 Backup Expansion (yearly growth)
$ 25,000 CISCO Smart Net
$ 2,500 San Switch Maintenance
$ 5,000 Overland Maintenance

721200 **Miscellaneous Expense (**$0) is recommended decreased $14,000 due to sales tax no longer calculated in the ConvergeOne Financial – Network Security Implementation Project lease.

721300 **Office Expense** ($17,000) is recommended increased $9,600 to fund the following:

$15,000 Back Up Tapes
$1,000 Office Supplies
$1,000 ISACA, Security Reading and Documentation

721307 **Office Furniture** ($2,000) is recommended increased $2,000 to fund the following:

$2,000 Office chairs – 4 New Employees

721314 **Computer Equipment** ($16,000) is recommended increased $9,000 to fund the following:

$16,000 New laptops – 4 New Employees

SERVICES & SUPPLIES (continued)

721400 **Professional & Specialized Services** ($651,395) is recommended increased $322,095 to fund the following:

*The significant growth in 00243-721400 is adding System Logging in the amount of $317,000 to this account. Please note, in Fiscal Year 2022-2023, System Logging was erroneously budgeted in 00243-721426. The increase in 00243-721400 is offset by a decrease in 00243-721426.

Professional Services – Recurring Costs

$7,000	Hard Drive Destruction
$16,000	External Consulting Services and Support
$800	ISACA Memberships
$61,250	Cisco Talos Incident Response
$35,000	Trace Digital Forensics Services - (increase of $7,000 due to increase Public Record Act requests and Email Audit requests)
$5,000	Insight Professional Services – Back Up Expansion
$68,845	Cloud Back Up -M365
$40,000	Internal Penetration Assessment
$317,000	*System Logging (In Fiscal Year 2022-23, this item was erroneously budgeted in 00243-721426)
$12,000	Meridian - Site Configuration
$35,000	ManageNow – Professional Services for Service Now
$19,500	Ransomware Protection

Professional Services – New Recurring Costs

$14,000	Data Center Cleaning
$20,000	Professional Services for Intune

721426 **Software** ($ 815,995) is recommended decreased $105,347 to fund the following:

$22,237	Manage Engine Active Directory Manager & Active Directory Audit Plus
$4,000	Admindroid
$25,000	Azure Cloud Security – MFA Tokens
$20,000	Secure File Solution
$22,000	Integrated Electronics Badge Software

SERVICES & SUPPLIES (continued)

721426 **Software (continued)**

$85,000	Internal Vulnerability Management & External Testing
$50,000	Server Infrastructure Network Management System
$20,814	Manage Engine Desktop Central and Patch Manager
$50,000	Network Infrastructure Monitoring & Mapping Maintenance
$4,000	Secure Password Manager Subscription Service
$28,044	Security Awareness Training
$275,000	Microsoft Enterprise Agreement
$10,600	SSL Certificate Renewal
$6,200	Pen Testing
$9,850	Training Subscription Fees
$49,000	Vendor Remote Access
$58,000	Enterprise Backup Software – Annual License and Maintenance
$5,000	Enterprise Backup Data DeDuplication Software
$20,000	Remote Access Mobile Device Management User and Device Licenses
$8,000	Remote Access Mobile Device Management Maintenance
$3,000	Deployment and Inventory Management
$3,600	Browser Security
$2,650	Certificate Tracking and Management
$30,000	Information Technology Service Management Licenses
$4,000	Batch Patch Software

721900 **Property Tax** ($18,000) is recommended increased $8,000 to fund the Property Taxes associated with the Network and Security Project Lease

722002 **Transportation & Travel** ($37,380) is recommended decreased $12,320 to fund training needs throughout the year.

$ 6,000	SANS Security
$20,540	Cisco Live
$5,190	RSA Training
$5,650	BlackHat USA

OTHER CHARGES

730302 **Rent** ($415,740) is recommended unchanged to fund the following capital lease:

$415,740 ConvergeOne Financial – Network Security Implementation Project (Final Payment -11/2028)

FIXED ASSETS

740301 **Equipment** ($145,000) is recommended increased $ 110,000 to fund the following:

End-of-Life (EOL) equipment indicates it has reached the end of its "useful life" and will no longer market, sell, or update. This introduces risk to the availability of the connectivity the device provides. In addition, the system becomes more insecure day by day leaving additional areas of vulnerability throughout the enterprise. The devices become more susceptible to being compromised and increases the security threat surface Countywide.

$ 30,000 Sheriff's Office Firewall Replacement – End-of-Life

The Sheriff's Office Firewall will reach end of life on 9/30/2025. This project is for the replacement of the hardware, configuration restoration and implementation of the devices to bring them up to date. This firewall is a Department of Justice security requirement.

Asset Tag Number: 30650
Age: 8 years (Purchased 7/21/2015)

$ 30,000 Courts Firewall Replacement – End-of-Life

The firewall between the County of Madera and the Madera Superior Court will reach end of life on 9/25/2025. This project is for the replacement of the hardware, configuration restoration and implementation of the devices to bring them up to date. This firewall is a security requirement.

Asset Tag Number: 30649 (a)
Age: 8 years (Purchased 7/21/2015)

FIXED ASSETS (continued)

740301 Equipment (continued)

$ 85,000 Firewall Management Console Replacement – End-of-Life

The Firewall Management Console (FMC) is used and required to manage, configure, and monitor the majority of our County firewalls. The County FMC will reach end of life on 7/31/2024. Once it reaches EOL, it will no longer receive software updates and security patches from Cisco. This puts our network at risk of security threats and potential operational issues.

To ensure the security and functionality of our network, it's necessary to replace the EOL FMC with a new one. The new FMC will provide improved security features, performance, and visibility into network traffic. It will also manage and monitor the latest Cisco firewall technologies, protecting our network against the latest security threats. Failure to replace our EOL FMC can result in potential security breaches, operational issues, and reputational damage. Therefore, replacing it is critical to maintaining the security and functionality of our network. This project is for the replacement of the hardware, configuration restoration and implementation of the device to bring them up to date.

Asset Tag Number: CL000045 (Invoice 9000199)
Age: 5 years (Purchased 9/19/2018)

COUNTY OF MADERA
BUDGET UNIT POSITION SUMMARY
BUDGET FOR THE FISCAL YEAR 2023-24

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

JCN	CLASSIFICATION	2022-23 Authorized Positions Funded	2022-23 Authorized Positions Unfunded	2023-24 Proposed Positions Funded	2023-24 Proposed Positions Unfunded	Y-O-Y Changes in Positions Funded	Y-O-Y Changes in Positions Unfunded	Notes
3387 3388	Network Security Engineer I or Network Security Engineer II	**1.0**	**-**	**5.0**		**4.0**	**-**	**A**
4121	Deputy CIO - Network & Security Services	**1.0**	**-**	**1.0**		**-**	**-**	
3387 3388 3389	Network Security Engineer I or Network Security Engineer II or Senior Network Security Engineer	**1.0**	**-**	**1.0**		**-**	**-**	
4222	Executive Assistant to the Dept Head	**1.0**	**-**	**1.0**		**-**	**-**	
	TOTAL	**4.0**	**-**	**8.0**	**-**	**4.0**	**-**	

NOTES:

A Reflects the request of the department to fund four (4) FTE Network Security Engineer I/II. The cost of the additional FTEs are funded through subvented departments