STATE OF CALIFORNIA

Budget Change Proposal - Cover Sheet

DF-46 (REV 07/23)

Fiscal Year 2025-26	**Business Unit Number** 7100	**Department** Employment Development Department
Hyperion Budget Request Name 7100-008-BCP-2025-GB		**Relevant Program or Subprogram** 5920, 5925

Budget Request Title

Continuation of Cybersecurity Staffing, Security Audit Logging and Data Security

Budget Request Summary

The Employment Development Department (EDD) requests $13.8 million ongoing and 29.0 positions funded equally between the General Fund and the Unemployment Disability Compensation Fund to continue support for its Cybersecurity Program. This funding will support the permanent extension of the cybersecurity resources that began in 2022-23, continued support for the movement of critical audit related data to a cloud solution, and maintain a secure Information Technology (IT) environment with Managed Detection and Response (MDR) services.

Requires Legislation (submit required legislation with the BCP) ☐ Trailer Bill Language ☐ Budget Bill Language ☒ N/A	**Code Section(s) to be Added/Amended/Repealed**	
Does this BCP contain information technology (IT) components? ☒ Yes ☐ No *If yes, departmental Chief Information Officer must sign.*	**Department CIO** Ajit Girn	**Date** 7/5/2024

For IT requests, specify the project number, the most recent project approval document (FSR, SPR, S1BA, S2AA, S3SD, S4PRA), the approval date, and the total project cost.

Project No.

Project Approval Document:

Approval Date:

Total Project Cost:

If proposal affects another department, does other department concur with proposal? ☐ Yes ☐ No

Attach comments of affected department, signed and dated by the department director or designee.

Prepared By Soma Widjaja	**Date** 7/5/2024	**Reviewed By** Jeffery Loverde	**Date** 7/5/2024
Department Director Nancy Farias	**Date** 8/21/2024	**Agency Secretary** Stewart Knox	**Date** 8/29/2024

Department of Finance Use Only

Additional Review: ☐ **Capital Outlay** ☐ **ITCU** ☐ **FSCU** ☐ **OSAE** ☐ **Dept. of Technology**

Assistant Program Budget Analyst Andrew March	**Date submitted to the Legislature** 1/10/2025

A. Problem Statement

EDD is one of the largest state departments with employees at service locations throughout the state offering a wide variety of services to millions of Californians through Job Service, Unemployment Insurance (UI), Paid Family Leave (PFL), State Disability Insurance (SDI), Workforce Investment, and Labor Market Information programs. EDD's benefit programs administer billions of dollars in benefits each year to provide financial stability to workers and communities. As California's largest tax collection agency, EDD also handles the audit and collection of payroll taxes and maintains employment records for more than 18 million California workers.

EDD's multi-billion-dollar benefit programs make it a high-value target for cybercriminals. The 2022 Budget included three-year limited-term funding to increase staffing resources within EDD's Cyber Security Division, purchase fraud-related risk management tools, invest in a data classification tool, and implement additional security assessment tools to reduce the risk of data breaches and improve EDD's overall cybersecurity posture. These efforts formalized EDD's cybersecurity management program by mitigating security findings, enhancing and replacing inadequate security solutions and controls, and securing data entrusted to the EDD and the State. Without continued support after 2024-25, EDD's programs, customers, employees, and data will become vulnerable to the landscape of cyber-attacks.

EDD safeguards the data and privacy of over 8,000 employees and millions of California citizens. This critical mission requires a robust cybersecurity posture to defend against ever-evolving cyber threats. MDR services play a vital role in EDD's cybersecurity framework. MDR provides incident investigation and response, threat detection, and threat hunting capabilities 24 hours a day, 7 days a week, 365 days a year. With this level of protection, EDD can better protect its critical assets and services during off hours, weekends, and on holidays.

Without continued staffing and the ability to modernize its security instrumentation and tools, EDD will be constrained in its ability to secure, monitor, and respond to advancing security threats. This would place California's most critical benefit and tax programs at risk of compromise. Since EDD's programs are needed the most during extreme economic downturns, the inability of EDD to protect these programs would have catastrophic impacts to California's most at-risk citizens.

The on-premises audit logging solution was procured utilizing funds appropriated within the 2019 Budget via EDD's Information Security Enforcement Team proposal. The core capabilities of this solution are broad scope log event collection/management, the ability to analyze log events and other data across disparate sources, and operational capabilities such as incident management, dashboards and reporting. Before the COVID-19 Pandemic, EDD utilized this on-premises solution to maintain these audit logs. When logs reached a certain age, they were changed to a "frozen" state for the remainder of the seven-year requirement. This on-premises solution was difficult to maintain and created challenges when retrieving data for audits, subpoenas, and investigations. It was costly to increase its storage and supporting it required very specific knowledge and skills that are difficult to recruit for.

In 2022-23, EDD moved its security audit logging solution from on-premises to the cloud because it is more scalable and allows for easier retrieval of older logs upon request. Continued funding for the cloud solution is requested to not only meet mandatory requirements for the California Department of Technology (CDT), Social Security Administration (SSA), Internal Revenue Service (IRS), and other control agencies, but also to continue to support ongoing fraud investigations, security incidents, and other requests from law enforcement entities.

Resource History
(Dollars in thousands)

Program Budget	**PY - 4**	**PY - 3**	**PY - 2**	**PY-1**	**PY***	**CY**
Authorized Expenditures	N/A	N/A	N/A	$10,158	$6,083	$6,083
Actual Expenditures	N/A	N/A	N/A	$3,454	$3,572	TBD
Revenues	N/A	N/A	N/A	N/A	N/A	N/A
Authorized Positions	N/A	N/A	N/A	29.0	29.0	29.0
Filled Positions	N/A	N/A	N/A	7.4	22.0	TBD
Vacancies	N/A	N/A	N/A	21.6	7.0	TBD

**Expenditure and encumbrance as of March 2024*

Workload History

Workload Measure	**PY - 4**	**PY - 3**	**PY - 2**	**PY-1**	**PY**	**CY**
Log Intake: the average volume of data that is sent to the Security Information and Event Management (SIEM) daily. **TB = Terabytes*	1 TB*/day	1 TB/day	2 TB/day	2.5 TB/day	3.5 TB/ day	4 TB/day

B. Justification

EDD is subject to mandatory information security requirements and undergoes regular audits from the CDT, the SSA, and the IRS. As such, EDD is required to retain certain application and security audit logs for a period of up to seven years. These logs include but are not limited to firewall, active directory, virtual private network, endpoint logs, web history, and any data for systems that process Federal Tax Information.

As a result of the COVID-19 Pandemic, EDD was met with an unforeseen and historic amount of Unemployment Insurance fraud. In order to investigate these fraudulent claims, certain logs were requested from the on-premises solution for periods of up to 2 years. Due to the limited storage capacities and technical limitations with the on-premises solution, most of these logs were already in the “frozen” state. As a result, retrieving these logs took several months, which further delayed response to fraud investigations and subpoenas from law enforcement and legal entities. To quicken response times to state and federal agencies, as well as law enforcement requests, EDD made the decision to move from on-premise to the cloud-based solution in 2022-23. This solution allows for greater storage capacity and quicker retrieval of “frozen” state logs.

Per the State Administrative Manual (SAM) Section 5335, "Each state entity is responsible for continuous monitoring of its network and other information assets for signs of attack, anomalies, and suspicious or inappropriate activities. Each state entity shall ensure:

- An event logging and monitoring strategy, which provides for audit trails and auditability of events and appropriate segregation and separation of duties.
- Event logging and log monitoring are performed with sufficient regularity that signs of attack, anomalies, and suspicious or inappropriate activities are identified and acted upon promptly.
- Sensors, agents, and security monitoring software are placed at strategic locations throughout the network.
- Situational awareness information from security monitoring and event correlation tools are monitored to identify events that require investigation and response.
- Potential security events are reported immediately to the security incident response team.
- Response to security event notifications from the Office of Information Security (OIS) and other third parties comply with the Security Event Notification and Response Protocols, Statewide Information Management Manual (SIMM) 5335-A."

EDD must comply with IRS Publication 1075 Section 4.3 Audit and Accountability AU-11, which states that entities must "Retain audit records seven years to provide support for after-the- fact investigations of incidents and to meet regulatory and organizational information retention requirements." This requirement exceeds capabilities provided by CDT Security Operations Center as a Service. To continue compliance with IRS Publication 1075, licensing and support of EDD's current security audit logging capabilities must continue, which requires permanent dedicated funding.

Per the Federal Information Security Modernization Act (FISMA), federal systems must meet minimum security requirements. As EDD utilizes SSA data, it is subject to FISMA requirements. FISMA suggests entities utilize National Institute of Standards and Technology (NIST) 800-53 controls. To continue compliance with FISMA and NIST 800-53, licensing and support of EDD's current security audit logging capabilities must continue, which requires permanent dedicated funding.

The California Cybersecurity Maturity Metrics capture many of the NIST Cybersecurity Framework sub-categories and a majority of the Foundational Framework (SIMM 5300-B). The metrics are reflective of NIST Cybersecurity Framework (CSF) categories: Identify, Protect, Detect, Respond, and Recover. The OIS has sponsored the state cybersecurity strategy that articulates that state departments/agencies are to align with the NIST cybersecurity framework. The resources requested will facilitate alignment with this OIS sponsored strategy. The framework categories are listed below, with examples of what they include (but are not limited to):

- Identify: Governance, data and system categorization, and vulnerability scanning
- Protect: Account management, encryption, and system configurations.
- Detect: Network and end-point monitoring.
- Respond: Incident response plans and testing.
- Recover: Technology recovery plans and testing.

Continued funding for cybersecurity staffing, consultant services, and cloud solution for security audit logs is critical for EDD to maintain service levels for its critical public-facing applications, ensure the security of EDD and constituent data, and meet audit requirements with the CDT, IRS, and other control agencies.

Staffing

This request includes ongoing funding for 29.0 positions to continue to facilitate Security Policy and Compliance, Risk Management and Analysis, Privacy, Litigation Support, eDiscovery, Disclosure, Cybersecurity Architecture, Fraud Detection/Prevention, Vulnerability Management, Application Security, Penetration Testing, Threat Cybersecurity System Engineering, Endpoint Security, Data Loss Prevention, and Access & Identity Management. The total cost of the staffing, including salaries and benefits, is $5.1 million annually. The following is the breakdown by classification of the 29.0 requested positions:

- 1.0 Career Executive Assignment (C.E.A.)
- 1.0 Information Technology (IT) Associate
- 4.0 IT Manager I
- 1.0 IT Manager II
- 9.0 IT Specialist I
- 12.0 IT Specialist II
- 1.0 IT Specialist III

Security Information and Event Management *(Cloud Licensing, Support Services, and Training)*

The SIEM solution provides the following critical security functions:

- Flexible data handling of analytics and a security compliance platform that provides visibility into who is accessing what data sets and systems.
- Customized watch lists that match compliance analysts' needs and priorities to provide quick visibility, insight, and monitoring into the activity that is happening within those systems so that malicious or noncompliant activities can be detected.
- Linking and analysis of user and entity activity to better inform security and compliance staff about threats, breach of information, and corresponding remediation.
- Threat hunting capabilities with a point-and-click interface that simplifies the process of creating complex search queries. Analysts will be able to quickly and easily engage in threat hunting by developing searches that otherwise may have been extremely difficult or impossible. The tool will remove the manual steps in threat hunting and provide automatic incident timelines instead of logs for rapid and proactive threat hunting.
- Log gathering to monitor network or system activity that is not "normal" or secure, which will enhance the ability to perform monitoring, initiate alerts, assist with defining compliance metrics, and train EDD staff with the use of these dashboards.
- Quick response to security events that will allow the security teams to react quickly to identify what is happening, stop the attack, and mitigate the damage.
- Simplification of the investigation process that will allow EDD to expand its capabilities for security application information, making security investigation faster and easier. In many cases, this will involve escalating only the most important information so that human staff can intervene, and when the staff does get involved, there is a consolidated place to correlate alarms from different tools and drill down to the root cause of attacks.
- Damage mitigation from attacks from quicker staff response and investigation.
- Minimization of false positives. False alarms are frequent throughout the current security suite of tools. These false positives eat into staff time that could be spent much more productively and may reduce response times to true emergencies.
- Fraud detection and prevention with GenAI to detect and analyze IP address and geo-spatial velocity or anomalies on vast amounts of data.
- Threat intelligence feeds and correlation of data with GenAI to identify emerging threats and vulnerabilities via indicators of compromise that are associated.
- Reduction in manual processes. Many staff spend a large portion of their day handling cumbersome manual tasks like updating firewall rules, adding new users, or de-provisioning users who have left the company. These sorts of repetitive tasks

are ideal for automation.

- Integration with IT operations tools that provide security analysts with the ability to integrate with asset databases, helpdesk systems, configuration management systems, and other IT management tools.

The ongoing Cloud Licensing, Support Services, and Training total $4.96 million.

Project Management *(Consulting Services)*
This contractor will assist in planning and refining system architecture, building reports/dashboards, and drafting Standard Operating Procedures. These consulting services will continue project management activities for the SIEM migration and integration activities, monitor standards and expectations to plan and deliver Cybersecurity initiatives, manage dedicated resources, track and report on progress, decisions, risks, and issues, and coordinate communication amongst teams and broader stakeholders. The contractor will also continue to identify roles and responsibilities needed to support new capabilities/service delivery models and establish a program to support staff through changes in process, structure, and expectations, as well as continue to develop and execute internal and external communications strategies to support stakeholders. These critical efforts require a dedicated full- time project manager as EDD does not currently possess the staff capacity to accommodate or assign to these efforts. This request will allow EDD to continue with the same project manager for the lifecycle of these active projects, which will allow for continuity of services and to prevent a disruption in project progress.

The project management services total $300,000.

Managed Detection and Response
MDR is an add-on to EDD's current Extended Detection and Response (EDR) platform, which offers 24/7 incident monitoring, containment, and response solutions with expertise on thousands of indicators of compromise and threat intelligence analyzed daily. While EDD's critical services, such as UI Online, SDI Online, and Accounting and Compliance Enterprise System, are available 24/7 to the public via the web, EDD staff is not available 24/7. The MDR contract is essential for maintaining a secure IT environment and protecting sensitive data and provides the following benefits:

- Cost-Effectiveness: Compared to building and maintaining an in-house MDR team with the required expertise, the MDR offers a cost-effective solution with proven scalability to accommodate a large department like EDD (8,000+ users, 30,000+ hosts).
- Enhanced Security Posture: The MDR augments existing security measures with continuous threat monitoring, expert analysis, and rapid incident response, significantly bolstering EDD's overall cybersecurity posture.
- Improved User Productivity: By proactively addressing security threats, the MDR minimizes security incidents and disruptions, allowing departmental staff to focus on their core tasks.
- Containment and Response: The MDR service provides services for containment and response exceeding and enhancing state staff capabilities of monitoring. This provides a level of assurance for the department unmatched by any other offering.

The ongoing MDR services total $2.5 million.

C. Departmentwide and Statewide Considerations

Having a centralized SIEM solution allows for EDD to store its critical security audit logs in a single system, allowing for easier retrieval of logs for incidents, security investigations, fraud investigations, subpoenas, and law enforcement requests. Continuity of the cloud solution is critical for EDD to maintain the growing number of logs, respond to requests timely, and meet various State and Federal requirements for audit logging capabilities. EDD requires these tools to maintain compliance with the following statewide directives, federal laws, and guidelines to safeguard EDD's information, data, and technology:

- Executive Order B-34-15 – Increase California's preparedness to respond to cyberattacks.
- Chapter 518, Statutes of 2015 (AB 670) – IT Security Assessments.
- Chapter 508, Statutes of 2016 (AB 1841) – Cybersecurity Incident Response Planning.
- California Department of Technology Strategic Plan – Vision 2023.
- Governor's Cal-Secure multi-year initiative.
- 20 Code of Federal Regulations section 603.9(b) (1): Requires unauthorized access and disclosure of Unemployment Compensation (UC) data.
- Internal Revenue Code section 6103(p) (4): Requires that agencies receiving federal tax information (FTI) comply with Publication 1075 -Tax Information Security Guidelines for Federal, State and Local Agencies.
- Civil Code section 1798.24(e): Requires agencies to keep an accounting of disclosures of personal information.
- SAM section 5330: Requires each state entity to ensure compliance with information security requirements, both internally and externally.
- SAM section 5335: Requires each state entity to continuously monitor its information systems for signs of suspicious or inappropriate activity.
- SAM section 5335.1: Requires each state entity to implement a continuous monitoring program to facilitate ongoing awareness of vulnerabilities and to support risk management decisions.
- SIMM section 5300-B: Foundational framework comprised of 30 priority security objectives to assist state entities with prioritization of their information security efforts.

D. Outcomes and Accountability

As the Cybersecurity Division continues to hire for the positions that were included in the Budget Act of 2022 (Chapter 43, Statutes of 2022), its reliance on professional services to maintain and operate the SIEM may decrease over time. During 2023-24, EDD made significant strides in recruiting and hiring for the positions. EDD continues to recruit for the remaining positions so that EDD's cybersecurity posture can become more resilient. With ongoing funding, EDD will continue to remain in compliance with State and Federal guidelines. Additionally, EDD will be able to best serve its customer base by adequately responding to incidents and fraud, and build additional rules, policies, and procedures to help prevent widespread fraud in the future.

The MDR contract will deliver the following positive outcomes:

- Reduced Risk of Data Breaches: Proactive threat detection and response minimize the likelihood of successful cyberattacks and data breaches.
- Faster Incident Response: Timely identification and containment of security incidents limit potential damage and expedite recovery efforts.
- Enhanced User Confidence: A secure IT environment fosters trust among employees and the public (including employers and employees across California).

E. Implementation Plan

- Continue to intake log sources that were unable to be added to EDD's SIEM solution - Ongoing.
  - Pending Applications – There is a combination of applications that were unable to be added to the on-premises environment as well as new applications that have been added to EDD's environment.
  - New EDD Applications – This will be an ongoing work effort as new applications are brought into the Department either by business need or as result of the EDDNext Project.
  - Examples of EDD applications that send logs to SIEM solution include but are not limited to:
    - External Applications: These are critical public-facing applications where the California constituents are file for services including:

        - UI Online: Where users can file and recertify for Unemployment Insurance benefits.
        - SDI Online: Where users can file for initial Disability Insurance and/or Paid Family Leave benefits.
        - E-Services for Business: Where employers can make tax payments, manage payroll tax accounts, and report new employees or contractors.
    - Internal Applications: These are applications internal to EDD that allow for the completion of critical day to day activities in support of EDD services including:
        - Firewall: These logs contain information for all traffic within EDD's network. These logs can be utilized not only for fraud and security investigations, but also to troubleshoot for performance and outages.
        - Access and Authentication: These logs contain data for all users that authenticate into EDD's critical systems and infrastructure, and contain critical elements for investigations such as timestamps, geolocation, and device information.

- Fraud Detection Program
    - Gather requirements from UI, DI, Tax, and Workforce Services business areas to determine what constitutes fraud.
    - Associate requirements with different types of log sources.
    - Perform gap analysis on current log sources and any unlogged sources that would be required because of the business requirements.
    - Consult with system owners for unlogged sources that need to be intake into the SIEM solution.
    - Create work plan for intake of new log sources.
    - Perform application integration with log sources.
    - Create detection rules, alerts, dashboards, reports, and retention policies.
    - Provide training to business and IT partners utilizing fraud detection data.
    - Provide ongoing analysis and support to EDD's executive management for awareness and further action as needed.

F. Supplemental Information (If Applicable)

N/A

BCP Fiscal Detail Sheet

BCP Title: Continuation of Cybersecurity Staffing, Security Audit Logging and Data Security

BR Name: 7100-008-BCP-2025-GB

Budget Request Summary

Personal Services

Personal Services	FY25 Current Year	FY25 Budget Year	FY25 BY+1	FY25 BY+2	FY25 BY+3	FY25 BY+4
Positions - Permanent	0.0	29.0	29.0	29.0	29.0	29.0
Total Positions	**0.0**	**29.0**	**29.0**	**29.0**	**29.0**	**29.0**
Earnings - Permanent	0	3,321	3,321	3,321	3,321	3,321
Total Salaries and Wages	**$0**	**$3,321**	**$3,321**	**$3,321**	**$3,321**	**$3,321**
Total Staff Benefits	0	1,818	1,818	1,818	1,818	1,818
Total Personal Services	**$0**	**$5,139**	**$5,139**	**$5,139**	**$5,139**	**$5,139**

Operating Expenses and Equipment

Operating Expenses and Equipment	FY25 Current Year	FY25 Budget Year	FY25 BY+1	FY25 BY+2	FY25 BY+3	FY25 BY+4
5301 - General Expense	0	62	62	62	62	62
5304 - Communications	0	39	39	39	39	39
5322 - Training	0	159	159	159	159	159
5324 - Facilities Operation	0	186	186	186	186	186
5326 - Utilities	0	11	11	11	11	11
5340 - Consulting and Professional Services - External	0	7,760	7,760	7,760	7,760	7,760
5344 - Consolidated Data Centers	0	62	62	62	62	62
5346 - Information Technology	0	36	36	36	36	36
54XX - Special Items of Expense	0	302	302	302	302	302
Total Operating Expenses and Equipment	**$0**	**$8,617**	**$8,617**	**$8,617**	**$8,617**	**$8,617**

Total Budget Request

Total Budget Request	FY25 Current Year	FY25 Budget Year	FY25 BY+1	FY25 BY+2	FY25 BY+3	FY25 BY+4
Total Budget Request	**$0**	**$13,756**	**$13,756**	**$13,756**	**$13,756**	**$13,756**

Fund Summary

Fund Source

Fund Source	FY25 Current Year	FY25 Budget Year	FY25 BY+1	FY25 BY+2	FY25 BY+3	FY25 BY+4
State Operations - 0001 - General Fund	0	6,878	6,878	6,878	6,878	6,878
State Operations - 0588 - Unemployment Compensation Disability Fund	0	6,878	6,878	6,878	6,878	6,878
Total State Operations Expenditures	**$0**	**$13,756**	**$13,756**	**$13,756**	**$13,756**	**$13,756**
Total All Funds	**$0**	**$13,756**	**$13,756**	**$13,756**	**$13,756**	**$13,756**

Program Summary

Program Funding

Program Funding	FY25 Current Year	FY25 Budget Year	FY25 BY+1	FY25 BY+2	FY25 BY+3	FY25 BY+4
5920 - Unemployment Insurance Program	0	6,878	6,878	6,878	6,878	6,878
5925 - Disability Insurance Program	0	6,878	6,878	6,878	6,878	6,878
Total All Programs	**$0**	**$13,756**	**$13,756**	**$13,756**	**$13,756**	**$13,756**

Personal Services Details

Positions

Positions	FY25 Current Year	FY25 Budget Year	FY25 BY+1	FY25 BY+2	FY25 BY+3	FY25 BY+4
1401 - Info Tech Assoc	0.0	1.0	1.0	1.0	1.0	1.0
1402 - Info Tech Spec I	0.0	9.0	9.0	9.0	9.0	9.0
1405 - Info Tech Mgr I	0.0	4.0	4.0	4.0	4.0	4.0
1406 - Info Tech Mgr II	0.0	1.0	1.0	1.0	1.0	1.0
1414 - Info Tech Spec II	0.0	12.0	12.0	12.0	12.0	12.0
1415 - Info Tech Spec III	0.0	1.0	1.0	1.0	1.0	1.0
7500 - - C.E.A. - C	0.0	1.0	1.0	1.0	1.0	1.0
Total Positions	**0.0**	**29.0**	**29.0**	**29.0**	**29.0**	**29.0**

Salaries and Wages

Salaries and Wages	FY25 Current Year	FY25 Budget Year	FY25 BY+1	FY25 BY+2	FY25 BY+3	FY25 BY+4
1401 - Info Tech Assoc	0	86	86	86	86	86
1402 - Info Tech Spec I	0	936	936	936	936	936
1405 - Info Tech Mgr I	0	497	497	497	497	497
1406 - Info Tech Mgr II	0	143	143	143	143	143
1414 - Info Tech Spec II	0	1,370	1,370	1,370	1,370	1,370
1415 - Info Tech Spec III	0	126	126	126	126	126
7500 - - C.E.A. - C	0	163	163	163	163	163
Total Salaries and Wages	**$0**	**$3,321**	**$3,321**	**$3,321**	**$3,321**	**$3,321**

Staff Benefits

Staff Benefits	FY25 Current Year	FY25 Budget Year	FY25 BY+1	FY25 BY+2	FY25 BY+3	FY25 BY+4
5150150 - Dental Insurance	0	19	19	19	19	19
5150200 - Disability Leave - Industrial	0	3	3	3	3	3
5150210 - Disability Leave - Nonindustrial	0	3	3	3	3	3
5150350 - Health Insurance	0	593	593	593	593	593
5150500 - OASDI	0	188	188	188	188	188
5150600 - Retirement - General	0	874	874	874	874	874
5150700 - Unemployment Insurance	0	20	20	20	20	20
5150750 - Vision Care	0	3	3	3	3	3
5150800 - Workers' Compensation	0	67	67	67	67	67
5150900 - Staff Benefits - Other	0	48	48	48	48	48
Total Staff Benefits	**$0**	**$1,818**	**$1,818**	**$1,818**	**$1,818**	**$1,818**

Total Personal Services

Total Personal Services	FY25 Current Year	FY25 Budget Year	FY25 BY+1	FY25 BY+2	FY25 BY+3	FY25 BY+4
Total Personal Services	**$0**	**$5,139**	**$5,139**	**$5,139**	**$5,139**	**$5,139**