

STATE OF CALIFORNIA
Budget Change Proposal - Cover Sheet
DF-46 (REV 07/23)

Fiscal Year 2024/25	Business Unit Number 2740	Department Department of Motor Vehicles
Hyperion Budget Request Name 2740-036-BCP-2024		Relevant Program or Subprogram All Programs

Budget Request Title
Cybersecurity Program Resources

Budget Request Summary

The DMV requests funding for five (5) new permanent positions, Information Technology (IT) security consulting services, and IT security tools to improve the Cybersecurity Program.

The requested resources will strengthen cybersecurity measures, expand State staff capabilities, reduce risk exposure, address compliance gaps with State mandated security requirements, and remediate security audit findings.

Requires Legislation (submit required legislation with the BCP) <input type="checkbox"/> Trailer Bill Language <input type="checkbox"/> Budget Bill Language <input checked="" type="checkbox"/> N/A	Code Section(s) to be Added/Amended/Repealed	
Does this BCP contain information technology (IT) components? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	Department CIO Prashant Mittal	Date 10/2/2023

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

Prepared By Steve Perry	Date 9/6/2023	Reviewed By Lee P. Scott	Date 12/20/2023
Department Director Steve Gordon	Date 12/22/2023	Agency Secretary Toks Omishakin	Date 12/23/2023

Department of Finance Use Only

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

Principal Program Budget Analyst Matthew Macedo	Date submitted to the Legislature 1/10/2024
---	---

A. Problem Statement

DMV employs nearly 10,000 public servants and provides essential services to millions of Californians. It is responsible for licensing drivers, registering vehicles, securing identities, and regulating the motor vehicle industry in pursuit of public safety. DMV serves customers online and in more than 187 field offices, 173 Auto Clubs, and over 6600 Business Partner locations across the state. The DMV generates \$14.0 billion of annual revenue and distributes approximately 86% of its collected revenue to local governments, law enforcement, and various state agencies.

Due to DMV's responsibility to serve the public's essential services, and its critical link in the State's revenue stream; it is imperative that DMV protect its service availability, information assets, and the public's personal information. It is also critical that DMV implement and maintain mandated security controls identified in various laws, regulations, directive, policies, and standards.

The DMV requests \$7.4 million FY 24/25, \$7.3 million in FY 25/26, and \$4.9 million in FY 26/27 and ongoing for five (5) new permanent positions, Information Technology (IT) security consulting services, and IT security tools to improve the Cybersecurity Program.

Table 1 Mandated Security Requirements

Reference	Description
CA Govt. Code §11549.3	State Security Program Duties
Cal-Secure Security Multi-Year Maturity Roadmap	Cybersecurity baseline capabilities
CA Information Practices Act §1798, et seq	Personal Information protection
Statewide Administrative Manual (SAM) 5300 Statewide Information Management Manual (SIMM)	State Security Policies/Standards
National Institute of Standards and Technology (NIST)	Security and Privacy Controls
Department of Justice (DOJ) IT Policy	Protect Criminal Justice Information
Payment Card Industry Data Security Standards (PCI-DSS)	Protect Credit card information

Failing to implement and maintain appropriate security measures increases the risk of a successful cyberattack and subsequent adverse impacts of:

- Reputational Damage
- Financial Loss
- Essential Service Disruption
- Legal Action

1. Cybersecurity Program Resources

DMVs existing resources are insufficient to meet, implement, and maintain required services and capabilities to protect and secure DMV information assets. Resource constraints are due to multiple factors which have steadily increased risk exposure.

- Compliance gaps due to continued and persistent findings across multiple security audits and assessments.
- Expanded attack surface due to modernization effort and technology transformation.
- New State-mandated security requirements and timeline for implementation.
- Increased complexity of the IT architecture due to expanded remote access capabilities for personnel and enhanced online services to the public.
- A continuously evolving threat landscape due to adversarial threat actors with sophisticated tactics are adept at infiltrating organizational information systems and obtaining personal information.

2. Compliance and Risk Exposure

DMVs current risk exposure is rated moderate due to 49 non-compliant findings. CA Govt. Code § 11549.3 require state-entities to undergo Information Security Program audits and Independent Security Assessments (ISAs.) The audits and independent security assessments (ISAs) are conducted respectively by the CA Department of Technology Office of Information Security (CDT-OIS) and the CA Military Department (CMD).

Table 1—Findings by Risk Severity

Very High	High	Moderate	Low	Very Low	Total
2	18	24	4	1	49

B. Justification

DMV requests \$7.4 million FY 24/25, \$7.3 million in FY 25/26, and \$4.9 million in FY 26/27 and ongoing for five (5) new permanent positions, Information Technology (IT) security consulting services, and IT security tools to improve Cybersecurity Program maturity. These additional resources are needed to comply with State mandated security requirements and address risks identified in various audit and assessment findings. Conforming to these additional requirements, in addition to the evolving changes to the threat landscape not only increases workload, but also requires establishing appropriate controls to protect DMV essential services and information assets. This proposal aligns with Cal Secure Roadmap initiatives to improve cybersecurity defense posture and reduce risk exposure.

The primary function of DMV's Information Security Services Branch (ISSB) is to protect DMV from cybersecurity threats, implement mandated security, as well as privacy requirements. The Chief Information Security Officer (CISO) establishes DMV Cybersecurity, Privacy and Risk Management Program strategy, while overseeing the 31 permanent employees who make up the branch. As DMV transitions to modern information technology infrastructure, security risks increase beyond the reach of the branch's authorized resources.

Staffing Increase Request

Evolving changes to the threat landscape and state-mandated security requirements necessitate additional resources to improve DMV cybersecurity defenses and reduce risk exposure of essential services and information assets.

The State CISO's response to the CSA Audit 2021-602 confirms the increasing cyber risk to state entities by stating " In the wake of the pandemic the cybersecurity threat landscape nearly quadrupled in the sophistication of attacks by nation state adversaries and criminal rings targeting every layer of our critical infrastructure."^[1] To strengthen cybersecurity defenses all reporting entities must implement the Cal-Secure Roadmap prioritized list of baseline cybersecurity capabilities over the next five years. At the close of each fiscal year, entities will be required to attest that they have achieved the required capabilities.

Upsurges of online transactions and web traffic increases DMV risk exposure. The top 10 security threats facing e-commerce include cyberattacks maliciously designed to disrupt website traffic and infect website applications with the sole purpose of obtaining personal information.

Permanent positions are needed to strengthen cyber security functions. These positions will increase DMV's ability to identify, protect, detect, respond, and recover from cyber events. This need is particularly evident for the SOC given their 24x7x365 responsibility to monitor attacks and defend against threat actors.

[1] [Report 2021-602 \(ca.gov\)](https://www.ca.gov/2021/06/24/report-2021-602/)

DMV requests the following new permanent positions to support critical DMV cybersecurity program components, address compliance gaps, and reduce reliance on IT security consultants. Annual staffing cost including salaries and benefits: \$666K in FY 24/25 and \$943K ongoing.

Table 2—PY Funding Cost Summary

Classification	Qty	FY 24/25 Cost	Annual Cost
PY Funding – Effective Date 07/01/2024 (Full year costs)			
Information Technology Manager II	1	\$139,000	\$139,000
Information Technology Specialist I	1	\$95,000	\$95,000
		(Half year costs)	(Full year)
Information Technology Specialist III	1	\$61,000	\$ 122,000
Information Technology Specialist II	1	\$56,000	\$113,000
Information Technology Specialist I	1	\$48,000	\$95,000
Staff Benefits		\$267,000	\$379,000
Total	5	\$666,000	\$943,000

Table 3—PY workload and functions of the requested positions.

a. Information Technology Manager II / Deputy Information Security Officer Duties	
<ul style="list-style-type: none"> • Program Manager <ul style="list-style-type: none"> ○ Identity Access Management ○ Integrated Risk Management 	<ul style="list-style-type: none"> • Incident Response Commander
b. Information Technology Specialist III / Principal Security Engineer Duties	
<ul style="list-style-type: none"> • Cloud Security Architect • Threat Intel / Hunting • Third Party Risk Management t 	<ul style="list-style-type: none"> • Integrated Risk Management Expert • Security Authorization & Assurance
c. Information Technology Specialist II / Integrated Risk Management Analyst Duties	
<ul style="list-style-type: none"> • Security Policy & Standards • Security Authorization • System Security Plans (SSP) 	<ul style="list-style-type: none"> • Vulnerability / Patch Mgmt. • Information Asset Ownership • Information Security Legislative Analysis
d. Information Technology Specialist I / Security Analyst – SOC (2.0 Positions) Duties	
<ul style="list-style-type: none"> • Anti-Malware Protection • Incident Response / Investigation • Log Management • Splunk Administration 	<ul style="list-style-type: none"> • 24/7 Continuous Monitoring • Monitoring & Alerts <ul style="list-style-type: none"> ○ Data Loss Prevention ○ Azure Security Events
e. Information Technology Specialist I / Security & Privacy Analyst Duties	
<ul style="list-style-type: none"> • Privacy Impact Assessments • Privacy Incident Investigation • Privacy Legislative Analysis 	<ul style="list-style-type: none"> • Enterprise Security & Privacy Awareness Training

IT Security Consulting Services

DMV requests funding to procure IT Security Consulting Services to address and assess compliance gaps, enhance staff knowledge, remediate audit findings, improve security processes, and implement security tools. This request supports the 2021 Cal-Secure initiative of people, process, and technologies to strengthen cybersecurity capabilities and reduce risk.

Table 4—IT Security Consulting Services

IT Security Consulting	FY 24/25	FY 25/26	Ongoing Costs
Security Risk Mgmt. Consulting	N/A	\$1,000,000	N/A
Web Application Testing - Permanent	\$175,000	\$175,000	\$175,000
Technology Recovery Planning (TRP) and Exercises	\$350,000	N/A	N/A
Security Architecture Assessment (Includes IDM)	\$500,000	N/A	N/A
IDM Development & Enhancement	\$800,000	\$800,000	N/A
NIST Cyber Security Framework (CSF) Assessment	\$350,000	N/A	N/A
Infrastructure Tools Implementation	\$500,000	N/A	N/A
Insider Threat Assessment	N/A	\$476,000	\$126,000
Total	\$2,675,000	\$2,451,000	\$301,000

IT Security Tools and Training

DMV requests additional funding for IT security tools and training to address audit and assessment findings and improve DMV Cyber Security posture. The tools will be used to enhance security awareness, identify, track, monitor assets, security threats, security events, and third-party risk.

Table 5—IT Security Training and Tools Cost Summary

IT Security Tools and Training	FY 24/25	FY 25/26	Ongoing Costs
IT Security Training	\$150,000	\$150,000	\$0
Network Operations Center Monitoring	\$850,000	\$850,000	\$850,000
Role Based Security Training	\$150,000	\$150,000	\$0
Email Security	\$390,000	\$390,000	\$390,000
Security Application Testing	\$150,000	\$150,000	\$150,000
Cloud Infrastructure Monitoring	\$250,000	\$250,000	\$250,000
Cloud Access Security Broker	\$175,000	\$175,000	\$175,000
Identity Management Orchestration & Provisioning	\$569,000	\$600,000	\$600,000
Privileged Account Management	\$600,000	\$600,000	\$600,000
Incident Response Management	\$480,000	\$480,000	\$480,000
Third Party Risk Management	\$200,000	\$200,000	\$200,000
Total	\$3,964,000	\$3,795,000	\$3,495,000

C. Departmentwide and Statewide Considerations

This proposal enables DMV to combat cybersecurity threats, safeguard essential services for the public, and protect privacy of personal information. This request aligns with the following State and DMV strategic plan goals.

1. Vision 2023 CA Technology Strategic Plan

- GOAL 1: Deliver easy-to-use, fast, dependable, and secure public services.

- GOAL 5: Build confident empowered multi-disciplinary teams.

2. DMV 2021-2026 Strategic Plan

- OBJECTIVE 1: Workforce

Foster a workforce and culture of innovation to make DMV a leader in talent attraction and retention.

- OBJECTIVE 2: DIGITAL SERVICES

Deliver simpler, faster ways to fulfill customer needs through expanded digital services.

- OBJECTIVE 3: TECHNOLOGY & DATA

Create flexible, secure technology systems to enable innovation and continuous improvement.

- OBJECTIVE 4: OPERATIONAL EFFICIENCY

Embed measurable efficiency in every aspect of the organization.

D. Outcomes and Accountability

The requested resources will allow DMV to support and maintain critical cybersecurity program components to protect state information assets from unauthorized access, operational downtime, data manipulation, and subsequent negative outcomes (e.g., data breaches, reputational damage, and data breach costs). These resources will improve DMV's cybersecurity defense posture, comply with mandated regulations, and address risks identified in various audit and assessment findings.

Approval of this request will support the 2021 Cal-Secure cybersecurity initiative of people, process, and technologies to reduce risk and will result in:

- Strengthened cybersecurity measures for California state government.
- Compliance with state and federal law, regulation, policies, and standards to protect the security and privacy of state information assets.
- Improved cybersecurity practices to identify, respond, and manage risk to state information assets.
- Reduced reliance on IT staff augmentation consulting services.
- Timely remediation of cybersecurity risks identified in the California Military Department Independent Security Assessments and CDT Office of Information Security Program Audits.
- Improved DMV cybersecurity capabilities including continuous monitoring, incident response, access management, phishing protection, vulnerability management, data loss preventions, threat protection, and risk management.
- Reduced risk of reputational damage, financial loss, or litigation due to essential service disruption or data breach. Increased staff to improve DMV Cybersecurity Program maturity. Expanded staff cybersecurity capabilities.

E. Implementation Plan

- **FY 2024/25 – Year 1**
 - Procure and Onboard Consultants
 - Execute Very/High Risk Remediation Activities
 - Procure and Implement Security Tools
 - Onboard New Permanent Positions

- Provide Core/Specialized Training to New Staff
- **FY 2025/26 – Year 2**
 - Procure and Onboard Consultants (Third Party NIST CSF Assessment/Security Testing)
 - Execute Moderate Risk Remediation Activities
 - Consultant Knowledge Transfer to State Staff
 - Web Application Security Testing with Focus on Digital Experience Project and Modernization Delivered Web Services
 - Third-Party NIST Cybersecurity Framework Assessment
 - Assess Remediated Findings for Sufficiency
 - Develop Follow-on Security Improvement BCP to Remediate Residual Gaps and Risks
- **FY 2026/27 – Year 3**
 - Continue Risk Remediation Activities
 - Assess Remediated Findings for Sufficiency

F. Supplemental Information

Table 6 – Total Costs

Requested Resources	FY 24/25	FY 25/26	Ongoing
IT Security Consulting, Tools, Training			
IT Security Consulting	\$2,675,000	\$2,451,000	\$301,000
IT Security Tools	\$3,664,000	\$3,495,000	\$3,495,000
IT Security Training	\$300,000	\$300,000	\$0
OE&E Standard Compliment	\$103,000	\$125,000	\$125,000
Subtotal	\$6,742,000	\$6,371,000	\$3,921,000
PY Classification / Quantity			
Information Technology Manager II (1.0)	\$139,000	\$139,000	\$139,000
Information Technology Specialist I (1.0)	\$95,000	\$95,000	\$95,000
	Half Year Costs	Full Year Costs	
Information Technology Specialist III (1.0)	\$61,000	\$122,000	\$122,000
Information Technology Specialist II (1.0)	\$56,000	\$113,000	\$113,000
Information Technology Specialist I (1.0)	\$48,000	\$95,000	\$95,000
Staff Benefits	\$267,000	\$379,000	\$379,000
Subtotal	\$666,000	\$943,000	\$943,000
Total by Year	\$7,408,000	\$7,314,000	\$4,864,000

BCP Fiscal Detail Sheet

BCP Title: Cybersecurity

BR Name: 2740-036-BCP-2024-GB

Budget Request Summary

	FY24					
	CY	BY	BY+1	BY+2	BY+3	BY+4
Salaries and Wages						
Earnings - Permanent	0	399	564	564	564	564
Total Salaries and Wages	\$0	\$399	\$564	\$564	\$564	\$564
Total Staff Benefits	0	267	379	379	379	379
Total Personal Services	\$0	\$666	\$943	\$943	\$943	\$943
Operating Expenses and Equipment						
5301 - General Expense	0	24	38	38	38	38
5304 - Communications	0	3	5	5	5	5
5320 - Travel: In-State	0	2	3	3	3	3
5322 - Training	0	301	316	40	40	40
5340 - Consulting and Professional Services - Interdepartmental	0	329	327	327	327	327
5340 - Consulting and Professional Services - External	0	4,195	3,953	1,912	1,912	1,912
5346 - Information Technology	0	1,888	1,729	1,596	1,596	1,596
Total Operating Expenses and Equipment	\$0	\$6,742	\$6,371	\$3,921	\$3,921	\$3,921
Total Budget Request	\$0	\$7,408	\$7,314	\$4,864	\$4,864	\$4,864

Fund Summary

Fund Source - State Operations

0044 - Motor Vehicle Account, State Transportation Fund	0	7,408	7,314	4,864	4,864	4,864
Total State Operations Expenditures	\$0	\$7,408	\$7,314	\$4,864	\$4,864	\$4,864
Total All Funds	\$0	\$7,408	\$7,314	\$4,864	\$4,864	\$4,864

Program Summary

Program Funding

2130 - Vehicle/Vessel Identification and Compliance	0	3,592	3,682	2,288	2,288	2,288
2135 - Driver Licensing and Personal Identification	0	2,316	2,271	1,535	1,535	1,535
2140 - Driver Safety	0	913	896	604	604	604
2145 - Occupational Licensing and	0	587	465	437	437	437

Investigative Services

9900100 - Administration	0	634	621	443	443	443
9900200 - Administration - Distributed	0	-634	-621	-443	-443	-443
Total All Programs	\$0	\$7,408	\$7,314	\$4,864	\$4,864	\$4,864

Personal Services Details

Positions	Salary Information									
	Min	Mid	Max	<u>CY</u>	<u>BY</u>	<u>BY+1</u>	<u>BY+2</u>	<u>BY+3</u>	<u>BY+4</u>	
1402 - Info Tech Spec I				0.0	2.0	2.0	2.0	2.0	2.0	
1406 - Info Tech Mgr II				0.0	1.0	1.0	1.0	1.0	1.0	
1414 - Info Tech Spec II				0.0	1.0	1.0	1.0	1.0	1.0	
1415 - Info Tech Spec III				0.0	1.0	1.0	1.0	1.0	1.0	
Total Positions				0.0	5.0	5.0	5.0	5.0	5.0	
Salaries and Wages	CY	BY	BY+1	BY+2	BY+3	BY+4				
1402 - Info Tech Spec I	0	143	191	191	191	191				
1406 - Info Tech Mgr II	0	139	139	139	139	139				
1414 - Info Tech Spec II	0	56	113	113	113	113				
1415 - Info Tech Spec III	0	61	122	122	122	122				
Total Salaries and Wages	\$0	\$399	\$565	\$565	\$565	\$565				
Staff Benefits										
5150150 - Dental Insurance	0	2	3	3	3	3				
5150200 - Disability Leave - Industrial	0	2	2	2	2	2				
5150350 - Health Insurance	0	62	83	83	83	83				
5150450 - Medicare Taxation	0	7	10	10	10	10				
5150500 - OASDI	0	30	41	41	41	41				
5150600 - Retirement - General	0	93	148	148	148	148				
5150800 - Workers' Compensation	0	21	26	26	26	26				
5150820 - Other Post-Employment Benefits (OPEB) Employer Contributions	0	17	22	22	22	22				
5150900 - Staff Benefits - Other	0	33	44	44	44	44				
Total Staff Benefits	\$0	\$267	\$379	\$379	\$379	\$379				
Total Personal Services	\$0	\$666	\$944	\$944	\$944	\$944				