CHAPTER 10

SOFTWARE

REVISED JUNE 2026

TABLE OF CONTENTS

ANNEXES

CHAPTER 10

SOFTWARE

1. PURPOSE. The purpose of this chapter is to establish policies and procedures for the effective management and use of software on CHP computer systems and network. The following policies and procedures apply software management best practices to mitigate the risk of fines for civil damages for copyright infringement, denial of product support or warranty service, and security vulnerabilities and/or breaches.

2. POLICY. In accordance with Sections 4846, California Software Management Policy; 4846.1, Software Management Plan; and 4846.2, Software Management Policy Reporting Requirements of the State Administrative Manual (SAM), the Department is required to establish appropriate software management policies, procedures, and practices to ensure all computer software used and/or purchased with state funds is procured legally and is used in compliance with licenses, contract terms, and applicable copyright laws. Software used and procured by the Department must meet applicable information security policies, as detailed in SAM Section 5300, Information Technology – Office of Information Security.

3. DEFINITIONS.

a. Commercial Off-the-Shelf Software. A software product ready-made for specific uses and available for sale to the public.

b. Conventional Artificial Intelligence. Data models that can be referred to as "machine learning," "data science," or any programming that is built for a few specific tasks, which are determined by the programmer. Artificial Intelligence (AI) does not produce or generate net-new content and can only analyze the data it is given.

c. Generative Artificial Intelligence. The class of AI models that emulate the structure and characteristics of data entered to generate content. This can include images, videos, audio, text, and other digital content.

d. Incidental Generative Artificial Intelligence Purchase. A purchase for which the Department identifies the use of Generative AI (GenAI) tools as part of the overall solution. A request to purchase a good or service for which GenAI assisted in the delivery is considered an incidental GenAI purchase.

e. Intentional Generative Artificial Intelligence Purchase. A purchase of a GenAI product or solution to meet a business need. A request to purchase a specific

GenAI product or solution at the onset of a procurement is considered an intentional GenAI purchase.

f. Open Source Software. Software that includes distribution terms that comply with the following criteria provided by the Open Source Initiative:

(1) Free Redistribution. The software can be distributed for free as part of a larger software package.

(2) Source Code. The code must either be distributed with the software or easily accessible.

(3) Derived Works. The code can be altered and distributed by the new author under the same license conditions as the product on which it is based.

(4) Integrity of the Author's Source Code. May restrict distribution of modified source code only if the license allows the distribution of patch files to modify the program at build time.

(5) No Discrimination Against Persons or Groups.

(6) No Discrimination Against Fields of Endeavor. Distributed software cannot be restricted on who can use it based on their intent.

(7) Distribution of License. The rights of the program must apply to all to whom the program is redistributed without need for an additional license.

(8) License Must Not Be Specific to a Product: An operating system (OS) cannot be restricted to be free only if used with another specific product.

(9) Restrictions. License must not impose restrictions on other software distributed alongside the licensed software.

(10) License Must Be Technology Neutral.

g. Platform as a Service. The capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, OSs, or storage, but has control over the deployed applications and possibly application-hosting environment configurations.

h. Software as a Service. The capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web

browser (e.g., web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, OSs, storage, or individual application capabilities, with the possible exception of limited user-specific application configuration settings.

4. ROLES AND RESPONSIBILITIES.

a. Information Management Division. Information Management Division (IMD) is the Office of Primary Interest (OPI) for all information technology (IT) activities of the Department. The IMD Chief is designated as the Department's Chief Information Officer (CIO) and is responsible for all IT infrastructure and IT assets. The IMD ensures all software assets are procured and managed in accordance with departmental and state procurement and software management policies and procedures.

b. Information Technology Governance Board. The Information Technology Governance Board (ITGB) is comprised of the CIO; Chief Technology Officer (CTO); Chief Enterprise Applications Officer; Information Security Officer (ISO); members of IMD, Information Technology Section (ITS), and Technology Infrastructure Section (TIS) management; and the Telecommunications Section and Communications Centers Support Section commanders. The ITGB is responsible for the review and approval of all requests for new nonstandard software to ensure the software is compatible with the Department's IT environment and IT policies and the proposed software is the appropriate IT solution to meet the business need.

c. Chief Technology Officer. The TIS commander is designated as the Department's CTO and is responsible for the enterprise architecture, including the evaluation and implementation of software on the Department's computer systems and network.

d. Project Management Group. The ITS, Project Management Group (PMG) is responsible for the development, maintenance, and implementation of the Department's Software Management Program, including, but not limited to, the following:

(1) Maintaining a list of approved software for use in the acquisition process and identifying unlicensed and unsupported software.

(2) Maintaining a baseline inventory of all Commercial off-the-Shelf (COTS) software.

(3) Performing ongoing inventory of all COTS software to ensure compliance with license agreements, terms, and conditions.

(4) Facilitation of software evaluations and presentation of the software evaluation team's analysis and recommendation to the ITGB.

(5) Monitoring approved software for upcoming GenAI functionality.

e. Technology Infrastructure Section, Customer Services Group. The TIS, Customer Services Group (CSG) is responsible for the following:

(1) Packaging and deploying software assets.

(2) Upgrading third-party software to new versions.

(3) Managing Active Directory (AD) groups and integrations.

(4) Ensuring all unlicensed, packaged software is removed from departmental devices.

(5) Granting access to third party software administered by CSG.

(6) Validating license availability.

f. Software Evaluators. Designated ITS, TIS, and Information Security Office staff are responsible for the evaluation of all new software requests to ensure the software meets the Department's IT standards, policies, and requirements and is compatible with the Department's overall IT environment.

g. Information Security Officer. The ISO is responsible for the Department's compliance with policies and procedures regarding the security of information and information processing assets. The ISO evaluates specific software to ensure it meets applicable security policies and standards and the use of the software either does not pose a security risk to the Department or the risk is at an acceptable level.

h. Privacy and Risk Management Administrator. The Privacy and Risk Management Administrator (PRMA) is responsible for the Department's Privacy and Risk Management Program, ensuring compliance with applicable laws and state policies and procedures. The PRMA conducts assessments of proposed IT solutions, identifies potential risks, and develops and implements risk mitigation strategies in coordination with OPIs.

i. Offices of Primary Interest.

(1) Identifying the need for nonstandard software, documenting the business justification and functional requirements, and submitting the request for IMD approval as described in paragraph 6.b. of this chapter.

(2) Providing information requested by IMD and/or ITS for the completion of the software evaluation.

(3) Assigning a point of contact to work with ITS in the completion of software audits.

(4) Ensuring software license and maintenance renewals are completed prior to term expiration.

(5) Ensuring compliance with all software approval conditions, as detailed in the IMD approval memorandum.

(6) Monitoring use of approved GenAI solutions to ensure compliance with approval conditions and acceptable use policy.

(7) Performing quality assurance of GenAI outputs to ensure GenAI models and vendors perform as expected.

(8) User management for third-party software not integrated with AD.

j. Business Services Section. Informing PMG via e-mail, at ITS_Admin@chp.ca.gov, when a supplier discloses the use of GenAI.

5. SOFTWARE CLASSIFICATIONS.

a. Standard Software. The TIS is responsible for support of the Department's OS and standard office suite (i.e., word processing, spreadsheet, database, presentation, diagram, and e-mail). Any enterprise software available for all departmental employees (e.g., Adobe Acrobat Reader) is also considered standard software.

b. Nonstandard Software. The OPIs are responsible for identifying the need for any software not currently included as part of the Department's standard software suite (e.g., Microsoft Visio and Project, Adobe Acrobat Pro and Creative Cloud, and Mark43 Records Management System) needed to support the OPI's business functions or programs. This includes freeware and any web-based software available for free on the Internet.

c. Custom Software. The ITS is responsible for maintaining and supporting all internally developed software applications (e.g., the Activity Tracking System, the Carrier Information Reporting and Evaluation System, the Project Tracking Log). To request the development of, or changes to, custom software, a CHP 53, Request for Information Technology (IT) Services, must be submitted through the

chain of command in accordance with Chapter 14, Information Technology Project Management and Oversight, of this manual.

6. NEW SOFTWARE REQUESTS. Commands may have a justifiable business need that cannot be met using existing departmental software resources. In such cases, commands must request approval of new standard or nonstandard software by submitting a ServiceNow Software Access & Request form, as described in paragraph 6.b. This allows IMD the opportunity to assess and evaluate the new software to ensure it aligns with the overall enterprise architecture and determine the implications, feasibility, IT requirements, and security of the proposed software.

Requests for new software shall be approved by IMD before the software is procured, installed, and/or accessed on departmental computing devices and/or network. All software, other than OS software for hardware, shall be evaluated by the ISO for security compliance and shall be approved by the CIO prior to procurement and/or use. This includes software that is a component of the procurement of any hardware or equipment and any new/additional modules for a previously approved software. (Refer to Annex A).

a. Submission Timeline. Commands are strongly encouraged to submit the new software request immediately following approval of the business justification and a minimum of one fiscal year prior to when the purchase requisition must be submitted to meet relevant deadlines (e.g., grant funding, purchase requisition submission). Should commands wait to submit the new software request until after funding is formally approved, IMD cannot guarantee approval will be granted prior to the fiscal year's IT procurement cut-off. For new software over $8,000,000, commands should submit the request a minimum of one year in advance of expected procurement execution to allow sufficient time for control agency approvals.

b. Submission Method.

(1) All new software requests must be submitted via the ServiceNow Software Access & Request form.

(2) Documentation (e.g., approved memorandum, e-mail approval) of the Division commander's approval of the request must be uploaded with the Software Access & Request form.

(3) Software requests will be evaluated and tracked for approval via the ServiceNow request. The following criteria will be considered:

(a) Software is to be installed on a "standalone" device that is not connected to the Department's network or is freeware accessed on the Internet or installed on a departmental device.

(b) Software does not collect, store, or transmit any sensitive or confidential data.

(c) Software does not require a Memorandum of Understanding (MOU) or Interconnection Security Assessment (ISA) between the Department and the vendor.

(d) Software does not require packaging for installation or integration with CHP's databases or systems.

c. Evaluation Process. Software selected for purchase and use by the Department must meet the requestor's functional requirements, have a successful past performance record, demonstrate mature software development capability and processes, meet applicable security standards and requirements, and be compatible with the Department's enterprise IT environment. The evaluation of software is to be performed by ITS, TIS, and ISO staff. (Refer to Annex C.) The following procedure shall be used when evaluating software:

(1) A software evaluation typically requires four to 14 months to complete. Depending on the complexity of the software and/or implementation, the following may be required:

(a) New Software Request for Information.

(b) Demonstration.

(c) Customer References.

(d) Software Trial or Proof of Concept.

(e) Proof of Value.

(f) System Security Questionnaire.

(g) Office of Primary Interest Questionnaire.

(h) Business Impact Assessment.

(i) Privacy Threshold Assessment. Identifies whether certain types of data (e.g., sensitive, confidential) are collected, stored, or transmitted.

(j) Privacy Impact Assessment. May be required based on the outcome of the Privacy Threshold Assessment.

(k) System Security Assessment. A more in-depth assessment may be required depending on the architecture of the software and any interconnected system.

(l) Generative Artificial Intelligence Risk Assessment. Required for procurement of incidental and intentional GenAI.

(m) California Department of Justice California Law Enforcement Telecommunications Systems Application. Required when changes to the Department's IT systems and infrastructure involve the California Department of Justice (DOJ) California Law Enforcement Telecommunications System (CLETS) or CLETS-derived data.

(n) Memorandum of Understanding. Used to record decision for roles and responsibilities when the Department accesses another state entity's or organization's IT resources when procurement is not needed.

(o) Interconnection Security Agreement. When procurement is not required, an ISA, typically accompanied by an MOU, details the technical process of how the data exchange will be achieved between the two entities, the security controls in place to protect the data, and the breach notification process should data be compromised at either entity.

(2) Proofs-of-Concept and Trials.

(a) Definitions.

1 Proof-of-Concept. A short-term, limited-scope exercise designed to validate the feasibility of a proposed software solution. Focuses on specific features, capabilities, or requirements, and is not intended for full-scale deployment.

2 Trial. A time-limited evaluation of a commercial product provided by a vendor to assess its functionality, useability, and suitability with the CHP operational environment and technical infrastructure. A trial may be provided by the vendor either at a cost to the Department or free of cost.

(b) A software Proof of Concept (POC) and/or trial may be conducted to evaluate the feasibility and suitability of a proposed software solution. (Refer to Annex D.)

(c) Software POCs and/or trials should be initiated in the fiscal year prior to the intended purchase of a software solution.

(d) Prior to initiating a POC and/or trial, the requesting command must:

1 Ensure the request to purchase the software and any associated implementation costs are included in the command's current or future spending plan.

2 Define the business requirements the proposed software is intended to address.

3 Conduct market research to identify possible solutions (e.g., attend trade shows or conferences, complete a Request for Information). Refer to the California Department of Technology's Market Research Guidelines at https://cdt.ca.gov/policy/market-research/ for additional guidance.

a During the market research process, the requesting command shall provide the same set of requirements and evaluation criteria to all vendors (at least three) to ensure fairness, consistency, and transparency in the selection process.

4 Obtain budgetary cost estimates for each option.

(e) All information outlined in paragraph 6.c.(2)(d) shall be submitted with documentation of the Division commander's approval (e.g., approved memorandum, e-mail approval) for ITGB review and approval. The ITGB will determine applicable technical and contractual requirements prior to approval of a POC and/or trial.

(f) If the OPI and ITGB determine a software POC and/or trial is necessary, the requesting command shall submit a ServiceNow Software Access & Request form for each proposed solution, maximum of two. The request shall clearly describe the business justification, concept/idea or requirements to be validated, and the "SMART" (specific, measurable, achievable, relevant, and time-bound) objectives to be achieved.

(g) To assess the Department's readiness, evaluate the effectiveness of the proposed solution, and determine the outcomes of the POC and/or trial, the requesting command will be provided the following documents to complete:

1 Business Readiness Questionnaire provided by IMD.

2 Proof of Concept/Trial Evaluation Questionnaire provided by IMD.

3 Privacy Threshold Assessment Questionnaire.

(h) Procurement Requirements.

1 The requesting command shall follow the applicable procurement rules and processes set forth in applicable SAM, Statewide Information Management Manual (SIMM), and departmental policies.

2 For software exceeding $8,000,000, including POC, trial, licensing, maintenance, and implementation, the OPI must:

a Verify whether the request falls within the definition of a California Department of Technology (CDT) project.

1/ If the request is considered a CDT project, the requesting command shall comply with the Project Approval Lifecycle or Project Delivery Lifecycle process in accordance with Chapter 14 of this manual.

2/ If the request is not considered a CDT project, confirm if it is available for purchase through a Department of General Services State Leveraged Procurement Agreement (LPA).

a/ If available, the requesting command must obtain quotes from the list of approved resellers.

b/ If not available, the requesting command must consult with the Purchasing Services Unit (PSU) to determine the appropriate procurement method and applicable requirements.

3 For software costing $8,000,000 or less, including POC, trial, licensing, maintenance, and implementation, the OPI must:

a Verify whether the product is available for purchase through an LPA.

1/ If available, the requesting command must obtain quotes from the list of approved resellers.

2/ If not available, the requesting command must consult with the PSU to determine the appropriate procurement method and applicable requirements.

4 If the POC and/or trial is provided at no cost, an MOU or ISA shall be established between the requesting command and the vendor prior to implementation. The MOU and/or ISA must be reviewed and approved by IMD prior to being sent to the vendor.

(i) Under no circumstances shall a software POC and/or trial commence prior to IMD approval and the full execution of the required MOU or contract.

(j) A software evaluation shall be conducted on the proposed solution(s) that meets the project's mid-level business requirements to ensure alignment with functional, operational, security, compliance, and compatibility standards. However, the requesting command shall select only one solution and conduct one software POC and/or trial at a time. If the selected product is unsuccessful, the requesting command may initiate a trial of the second evaluated product with approval from IMD.

(k) Prior to the POC and/or trial beginning, the requesting command and IMD will collaboratively document "SMART" (specific, measurable, achievable, relevant, and time-bound) objectives by which to measure success of the POC and/or trial.

(l) The requesting command shall ensure all documentation is complete and accurate prior to submission and shall serve as the primary point of contact during the POC and/or trial period. The command shall monitor progress, track findings, and document results for review.

(m) The IMD shall oversee the POC and/or trial process, provide guidance on technical requirements, and ensure compliance with applicable SAM, SIMM, federal, state, and departmental policies.

(n) Any POC and/or trial software requiring installation on departmental devices may only be installed for testing in pre-production environments to protect the integrity of the Department's production systems and infrastructure.

(o) Any POC and/or trial software requiring integration with the Computer Aided Dispatch (CAD) system, its data, or inclusion of any CLETS or CLETS-derived information is excluded from the POC/trial process until additional analysis, scoping, and approvals are completed.

1 Should the integration or inclusion of CAD be required or desired, a separate scoping request and subsequent scoping meeting will be required.

2 An application to the DOJ may be required as it relates to the application/system's proximity to CAD, CLETS, and/or CLETS-derived data.

a If a complete application to DOJ is required, the timeline for implementation of the software will be extended and may impact the POC and/or trial as determined by the scoping meeting and initial inquiry to DOJ.

3 Should any integration with the Department's Geographical Information System environment be desired or required, including map layers and related data, a separate scoping request and subsequent scoping meeting will be required to determine level of effort and feasibility.

4 All integrations mentioned above may require additional funding that will need to be acquired by the requesting OPI and allocated to the project.

(p) Under no circumstances shall POC and/or trial software be deployed or operated within a production environment unless formal approval has been obtained from the ITGB, ISO, CIO, and the commander of the requesting command. Approved testing shall only be conducted within the CDT's controlled sandbox environment.

(q) When the agreed upon POC and/or trial period has ended, the software shall be uninstalled/disconnected from all departmental end points. It is the requesting command's responsibility to ensure end user compliance with the terms of the POC and/or trial.

(r) Upon completion of the POC and/or trial, the requesting command shall prepare a POC and/or trial summary, in coordination with the OPI and IMD, documenting the results, lessons learned, and recommendation for next steps, including whether to pursue full implementation or to continue evaluating other alternative solutions.

(3) Project Approvals. In addition to the Department's software evaluation process and IMD approval, the implementation of a new software may meet criteria requiring California State Transportation Agency and/or CDT approval prior to procurement and implementation. See Chapter 14 of this manual for more information regarding CDT's Project Approval Lifecycle.

7. GENERATIVE ARTIFICIAL INTELLIGENCE.

a. Approved Use Cases. Generative AI solutions for use cases identified by requesting commands will be assessed by IMD for approval on a case-by-case basis.

b. Assessment. Software leveraging GenAI technology and use cases will be assessed and approved in accordance with current state policy, as established by CDT.

(1) Incidental Generative Artificial Intelligence. The SIMM 5305-F, Generative Artificial Intelligence Risk Assessment, will be completed upon disclosure of GenAI technology either during the software evaluation process or during the procurement process.

(2) Intentional Generative Artificial Intelligence. The SIMM 5305-F, and, if classified as moderate or high risk, a CDT consultation, must be completed prior to release of the solicitation.

c. Procurement. Under no circumstances are procurements for intentional or incidental GenAI to be executed prior to completion and approval of the SIMM 5305-F and, if required, the CDT consultation.

d. Acceptable Use. Use of approved GenAI solutions/technologies must comply with Chapter 18, Acceptable Use Policy, of this manual.

e. Functionality Added Mid-Contract Term. In the event a software publisher adds GenAI functionality mid-contract term, the OPI and IMD will collaborate to complete the SIMM 5305-F. Depending on the business need for the software and risk to the Department, IMD may require the following:

(1) Generative AI functionality be disabled until the assessment is completed and approved by IMD.

(2) If the GenAI functionality cannot be disabled, poses an unacceptable risk to the Department, and/or cannot be appropriately mitigated, IMD may require users discontinue use of the software completely until an acceptable solution can be identified.

8. SOFTWARE MANAGEMENT.

a. Virus Protection. Commands shall be aware of the risks associated with the introduction of new software or files on departmental assets. All software and/or files shall be checked for viruses using the Department's virus protection software before installation on any CHP device. (Refer to Chapter 5, Malware Prevention and Protection, of this manual for additional information.) Laptop and tablet users

must connect their device to the CHP network and log in at least every 60 days to update the virus software definitions.

b. Software Version Control. If a nonstandard software is a COTS product and purchased through the standard procurement process, the OPI shall perform the initial research to determine the appropriate software version. The ITS will review and provide final approval of the software version to be deployed to a production environment. The ITS will also make the final determination for internally developed custom applications. Should the version of existing nonstandard software require an update, commands must complete the following:

(1) If the update is purchased via purchase requisition, it must be delivered to ITS, via e-mail, at ITS_Admin@chp.ca.gov. The ITS will open a ServiceNow work order for the packaging and installation of the new version via Microsoft Software Center.

(2) If the software update is included as part of purchased software maintenance, commands must open a work order via ServiceNow and attach any links/instructions received. The new version will be packaged for installation via Microsoft Software Center.

c. Software Education and Training. The OPI and ITS staff will conduct joint testing of new applications to become familiar with the basic, advanced, and unique features of each application. Upon completion of this process, user-level operational instructions will be created by the OPI. These instructions will be available to all personnel during scheduled training and published on the CHP Intranet site as needed.

d. Software Management and Compliance. The Department is responsible for developing, implementing, and maintaining specific plans, procedures, and processes to ensure compliance with established state requirements, collectively referred to as the Software Management and Compliance Program (SMCP). The SMCP documents the policies, software governance structure, roles, and responsibilities, as well as the internal processes that support the SMCP.

e. Software/Application Installation. The Department utilizes software packaging software to install and deliver software and applications to the device or user. This network service installs software/applications on devices and repairs the installations should they become damaged. It also allows software/application delivery by group membership and provides the ability to restrict the use of a software or application for security reasons or business needs. When new software/applications are approved and purchased, they must be delivered to the ITS Acquisition Services Unit, via e-mail at ITS_Admin@chp.ca.gov, so the software/application can be packaged. The TIS Enterprise Administrators Unit is

responsible for packaging software/applications. This package can then be used to install the software/application on as many devices for which there is a business need and licenses available. The original software/application shall be stored in the Department's software repository. All devices must be connected to the CHP network to install software/applications.

f. Software Renewal. The OPI is responsible for ensuring software licenses and required maintenance do not expire. On-premises software will be managed by the OPI in coordination with ITS. The software life cycle should be reviewed for cost, upgrade, and replacement factors. The ITS shall be consulted immediately if a decision is made to not renew software licenses currently in use.

g. Software Disposal. Software retirement will occur on an as-needed basis as determined by the OPI and ITS. If it is determined nonstandard software will not be renewed or is no longer being used, a request to remove and/or uninstall software should be submitted to the TIS, IT Support Unit via ServiceNow. The TIS will coordinate with the OPI to ensure proper removal from all devices and proper disposal of any software media.

9. REQUEST TO USE SOFTWARE. To request access to and/or the installation of custom or nonstandard software, the user must submit the Software Access & Request form via ServiceNow. The request will be routed to the user's supervisor for review and approval. (Refer to Annex B.)

10. COPYRIGHT PROTECTION AND ENFORCEMENT.

a. Illegal Software. Employees shall not install unauthorized or illegal software on any Department-owned device or network workstation. Illegal software includes software not licensed for use by the Department.

b. Copyrighted Software. Employees shall not copy or share copyrighted software. Copyrighted software is proprietary software to which a software publisher, business, or person owns all intellectual property rights.

c. Copyrighted Files. Employees who download copyrighted files (e.g., graphics, sound files) from the Internet, or any other remote resource, are reminded it is unlawful to use such files without the expressed permission of the owner.

d. Software and Information Industry Association.

(1) The Software and Information Industry Association (SIIA) is a nonprofit trade organization for the software and digital content industry. The SIIA's mission is to provide information to and protect and promote the industry. As

part of their mission to protect the industry, SIIA receives permission from its members to enforce their software copyrights and trademarks.

(2) Under Title 17, Chapter 5, Copyright Infringement and Remedies, of the United States Code, the fines and penalties for copyright infringement can be severe and may result in civil and/or criminal action.

11. USE OF OPEN SOURCE SOFTWARE.

a. The use of Open Source software on departmental computer systems may be acceptable under certain circumstances in which a business need has been identified and cannot be reasonably met by standard software or the purchase of suitable nonstandard software is not possible. To request the use of any Open Source software, commands shall submit a new software request via ServiceNow, as described in paragraph 6. of this chapter.

12. USE OF PERSONALLY OWNED SOFTWARE.

a. The use of personally owned software on departmental devices or the CHP network is strictly prohibited.

b. Screensavers and/or Wallpapers. The installation of personally owned or third-party screensavers and/or wallpapers is prohibited. Many commercially available products are both hard disk and memory intensive and may affect the performance of the device.

13. USE OF DEPARTMENTAL SOFTWARE ON HOME DEVICES. Official Department business should be conducted on departmental assets only. Installation of the Department's software on personally owned home computing devices is not permitted. Use of Software as a Service products on personally owned home computing devices is not permitted, with the exception of Microsoft Office 365.

14. DATA ENCRYPTION.

a. Definition. Data encryption is the process of scrambling data so it appears to be random, unintelligible information. Encryption prevents any nonauthorized party from reading or changing data by converting plain text (English or any other language) into cipher text (unintelligible information). Once the data is encrypted, a password or key is required to decrypt the data back to its original form.

b. Policy. Departmental data must be protected by approved data encryption software installed on all devices. Employees shall not use any personal encryption software on departmental devices.

c. Roles and Responsibilities.

(1) The ISO is responsible for approving encryption software, monitoring reports pertaining to the audit log, and establishing security policies and user properties.

(2) The TIS is responsible for the installation, configuration, maintenance, and updates of encryption software, as well as the equipment the software resides on. The TIS issues and revokes encryption certificates in accordance with the criteria identified in this chapter.

(3) The Internal Affairs Section (IAS) shall provide its own administrator to be responsible for issuing and revoking user encryption keys for IAS personnel only. The IAS has the ability to decrypt all departmental communications.

(4) The Computer Crimes Investigation Unit (CCIU) shall provide its own administrator to be responsible for issuing and revoking user encryption keys for CCIU personnel only. The CCIU has the ability to decrypt all departmental communications.

d. Exceptions.

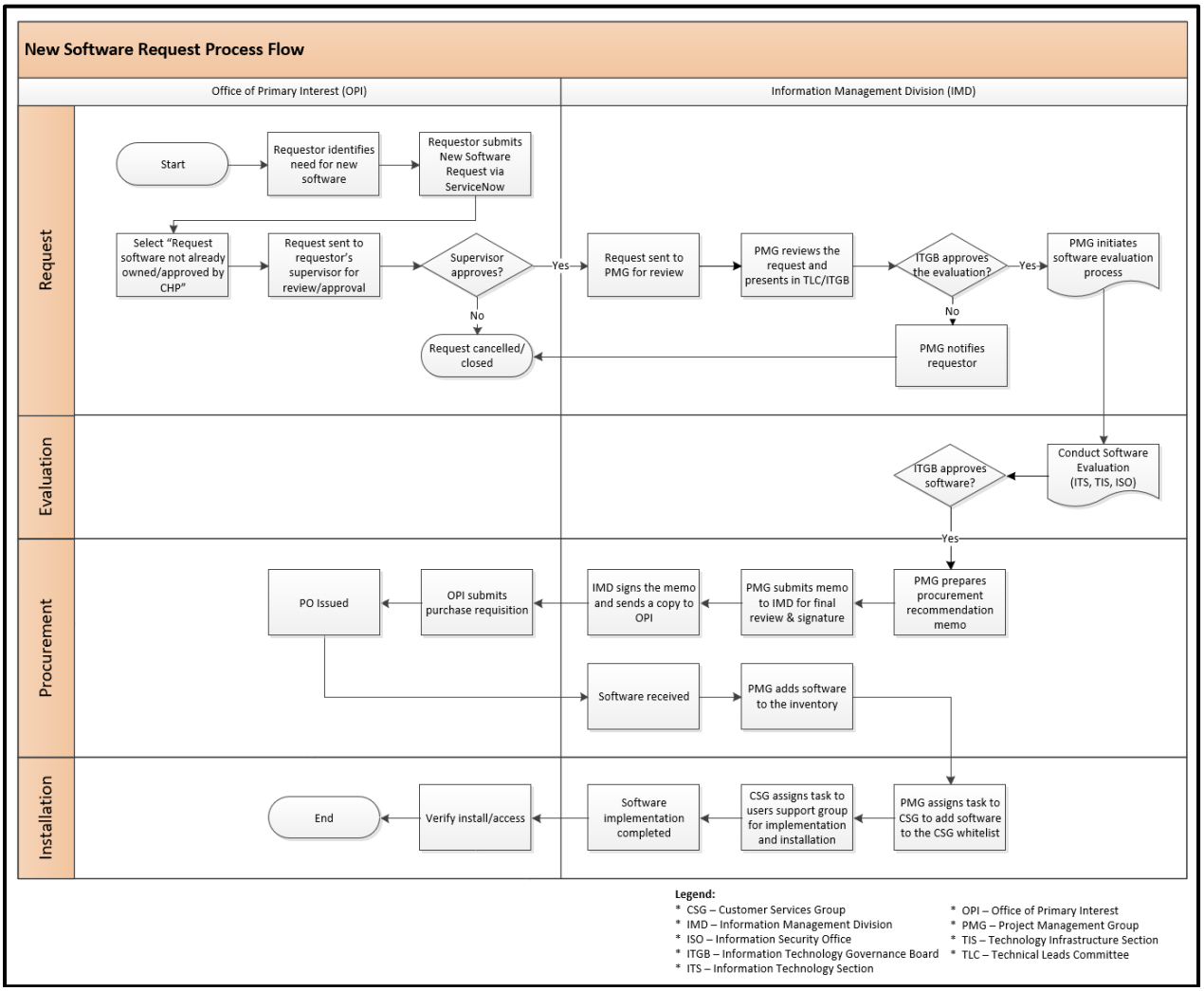
(1) To request the use of data encryption software other than the departmental standard, the requesting command shall submit a New Software Request for approval as described in paragraph 6. of this chapter and include a thorough justification of the business need.

(2) To request exemption from the use of data encryption software, a memorandum shall be submitted through channels to the ISO for review and approval and must include a thorough justification of the business need. Upon ISO approval, the request will be forwarded to the ITGB for approval.

THIS PAGE INTENTIONALLY LEFT BLANK

ANNEX A

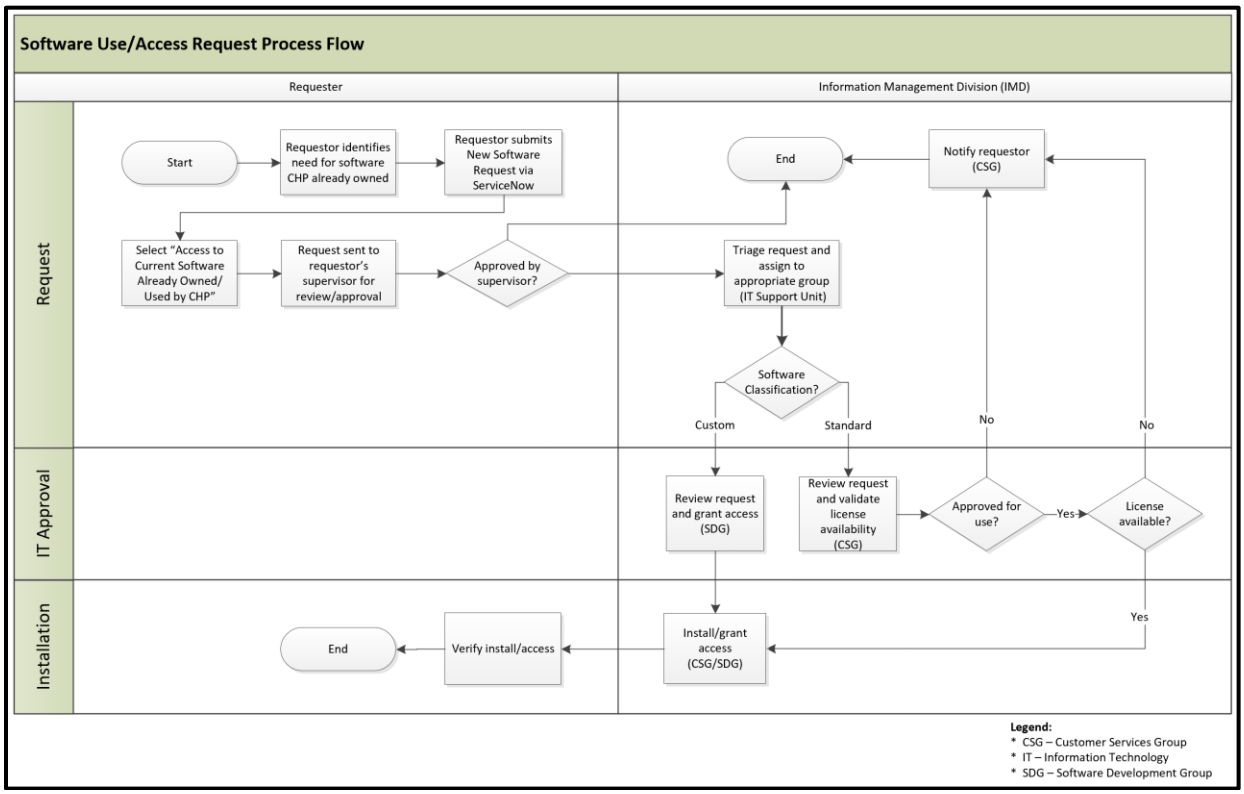
NEW SOFTWARE REQUEST PROCESS FLOW



THIS PAGE INTENTIONALLY LEFT BLANK

ANNEX B

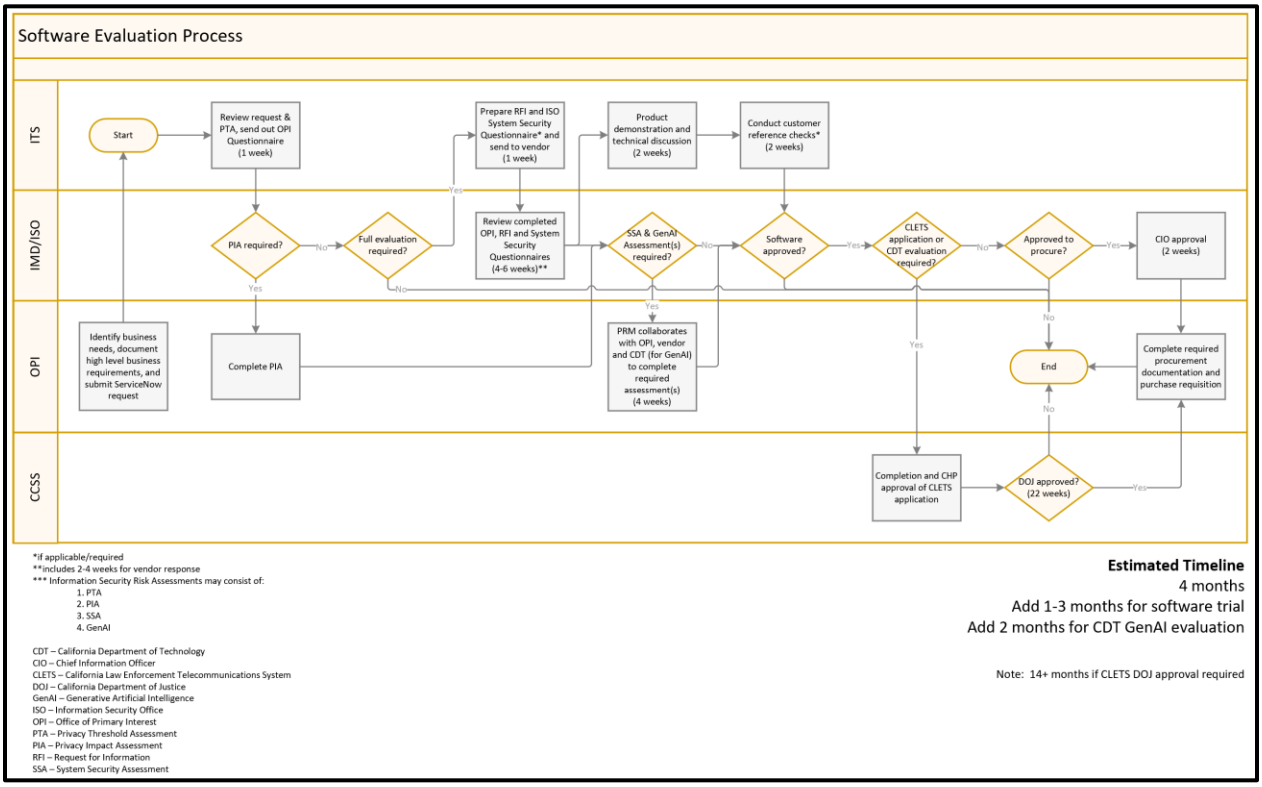
SOFTWARE USE/ACCESS REQUEST PROCESS FLOW



THIS PAGE INTENTIONALLY LEFT BLANK

ANNEX C

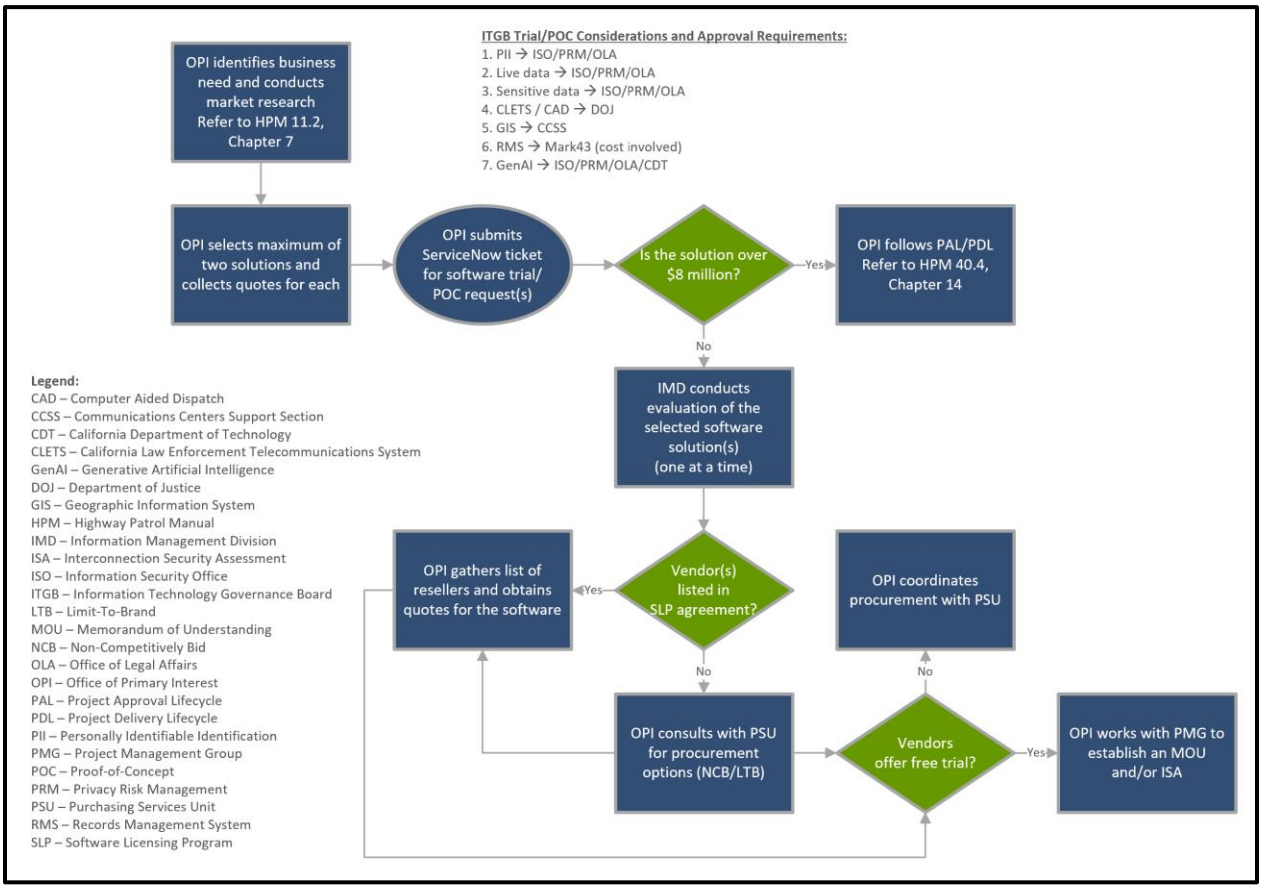
SOFTWARE EVALUATION PROCESS



THIS PAGE INTENTIONALLY LEFT BLANK

ANNEX D

SOFTWARE TRIAL/PROOF OF CONCEPT REQUEST WORKFLOW



THIS PAGE INTENTIONALLY LEFT BLANK