

STATE OF CALIFORNIA
Budget Change Proposal - Cover Sheet
 DF-46 (REV 08/15)

Fiscal Year 2016-17	Business Unit 4170	Department California Department of Aging	Priority No. 1
Budget Request Name 4170-001-BCP-BR-2016-GB		Program 9900100 & 9900200 ADMINISTRATION AND DISTRIBUTED ADMINISTRATION	Subprogram

Budget Request Description
CDA IT Branch Staffing

Budget Request Summary

The California Department of Aging (CDA) requests authority for 3 PYs. The proposal uses \$423,000 in existing expenditure authority for its Information Technology Branch to bring staffing up to the minimum level necessary to meet State IT requirements, ensure a stable network environment and mitigate security concerns to an acceptable level. This request will be funded using a combination of existing CDA funding sources including Older Americans Act federal funds and Medi-Cal (General Fund and FFP).

Requires Legislation <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Code Section(s) to be Added/Amended/Repealed	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 <i>If yes, departmental Chief Information Officer must sign.</i>	Department CIO <i>Ken Ketschever</i>	Date <i>8-25-15</i>
For IT requests, specify the date a Special Project Report (SPR) or Feasibility Study Report (FSR) was approved by the Department of Technology, or previously by the Department of Finance. <input type="checkbox"/> FSR <input type="checkbox"/> SPR Project No. Date:		

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 <i>Cynthia R.</i>	Date <i>8/25/15</i>	Reviewed By <i>Frank Hansen</i>	Date <i>8-25-15</i>
Department Director <i>Tom Connolly</i>	Date <i>8/25/15</i>	Agency Secretary <i>Mark Vinig for</i>	Date <i>8/27/2015</i>

Department of Finance Use Only	
Additional Review: <input type="checkbox"/> Capital Outlay <input type="checkbox"/> ITCU <input type="checkbox"/> FSCU <input type="checkbox"/> OSAE <input type="checkbox"/> CALSTARS <input type="checkbox"/> Dept. of Technology	
BCP Type: <input type="checkbox"/> Policy <input type="checkbox"/> Workload Budget per Government Code 13308.05	
PPBA <i>[Signature]</i>	Date submitted to the Legislature <i>1/7/16</i>

Analysis of Problem

A. Budget Request Summary

The California Department of Aging requests authority for 3 PYs. This proposal uses \$423,000 in existing expenditure authority for its Information Technology Branch to bring staffing up to the minimum level necessary to meet State IT requirements and increased workload, ensure a stable network environment and mitigate security concerns to an acceptable level. This request also includes an upgrade to the Department's CIO to a DPM III. This request will be funded using a combination of existing CDA funding sources as shown in the table below.

FUND SOURCES	
GENERAL FUND	\$154,000.00
FEDERAL FUND (OAA)	\$102,000.00
REIMBURSEMENT FROM MEDI-CAL (FFP)	\$149,000.00
REIMBURSEMENT FROM OTHER PROGRAMS	\$14,000.00
SPECIAL FUNDS	\$4,000.00
TOTAL	\$423,000.00

B. Background/History

As the federally designated State Unit on Aging, CDA administers funds allocated under the federal Older Americans Act and the Older Californians Act and through the Medi-Cal program. CDA contracts with a statewide network of 33 Area Agencies on Aging (AAA), who directly manage a wide array of federal and state-funded services that: help older adults find employment; support older and disabled individuals to live as independently as possible in the community; promote healthy aging and community involvement; assist family members in their vital caregiving role; and advocate on behalf of residents in long-term care (LTC) facilities. Each AAA is responsible for service delivery in geographic service regions known as Planning Service Areas (PSA).

Through interagency agreement with the Department of Health Care Services (DHCS), CDA also administers the Multipurpose Senior Services Program (MSSP) and certifies licensed Adult Day Health Care (ADHC) centers as Medi-Cal Community-Based Adult Services Program (CBAS) providers.

The CBAS program monitors 241 CBAS centers serving 32,000 Medi-Cal participants statewide. CBAS activities require considerable IT support related to applications review and processing, onsite surveys and documentation, extensive data collection and analysis, mandated reporting and data sharing, and tracking adverse and corrective actions. New requirements associated with the 1) Affordable Care Act (ACA) Provider Enrollment screening process, 2) the CMS Home and Community-Based Settings (HCBS) Regulations, and 3) the updated 1115 Waiver are creating an increase in CBAS workload. In addition, the expiration of the State Settlement Agreement that guided the transition of CBAS to managed care and the expiration of the State moratorium on new ADHC/CBAS licensees will significantly increase the volume of CBAS licensing and survey work. All of these developments significantly increase the need for IT support.

The MSSP Branch oversees the programmatic and administrative elements of local MSSP site operation through monitoring activities, formal on-site Medi-Cal Utilization Reviews (URs), policy directives, and technical assistance. An IT application supports some of the Branch's work activities, but slow manual processes used for the last 20 years are still needed to meet requirements. Currently, there is only limited electronic data validation, error identification and correction, and reporting capability.

Staffing History

CDA's IT Branch has been minimally staffed over the years and has never been augmented to keep up with workload associated with major technological changes, especially in the area of security-related requirements and reporting to control agencies about them. At the same time, budget cuts have resulted in the loss of IT resources and positions. Currently the Branch has only 7.0 PYs.

Analysis of Problem

Resource History (Dollars in thousands)

Program Budget	PY – 4 2010-11	PY – 3 2011-12	PY – 2 2012-13	PY – 1 2013-14	PY 2014-15
Authorized Expenditures	497,074	453,735	418,921	429,597	427,551
Actual Expenditures	349,361	397,045	402,752	422,406	TBD
Revenues	0	0	0	0	0
Authorized Positions	7.0	6.0	6.0	6.0	6.0
Filled Positions	4.9	5.8	6.0	5.9	6.0
Vacancies	2.1	0.2	0	0.1	0

Workload History

Workload Measure	PY – 4 2010-11	PY – 3 2011-12	PY – 2 2012-13	PY – 1 2013-14	PY 2014-15	CY 2015-16
PC Patch Schedule dedicated hours	12	12	6	6	12	12
Threat Monitoring dedicated hours	0	12	3	4	6	12
Department Computers Encryption percentage	18%	23%	25%	28%	31%	34%
Technology Recovery Planning and backup percentage completed	80%	40%	20%	20%	20%	35%

C. State Level Considerations

As much as possible, CDA is participating in State- and CHHS-level IT initiatives that seek efficiencies and decreased costs through strategies such as enterprise shared services; cloud services; project collaboration; common solutions; group purchasing; leveraged resources; and better planning and oversight of project lifecycles. While all of these approaches are aimed at reducing costs to the State and increasing security in the long run, in the short run, successful and appropriate implementation requires that each department contribute even more time, resources, and staff on top of their regular duties.

For example, CDA is working with sister departments within CHHS Agency to identify existing network infrastructures that can be leveraged by CDA. "Piggy-backing" on another department's network investment would allow CDA to spend less to bring our infrastructure up to standards by tapping into a solution that already exists. However, coordinating such an arrangement and transitioning CDA to these leveraged resources involves additional staff time and expertise that CDA does not have.

Additional upfront staff resources will be required to migrate basic services, such as web servers, file servers, and other applications, into the CalCloud environment (Technology Letter 14-04). If determined cost-effective for CDA, transition to an already secure and stabilized environment will save CDA in the long run and provide better security, offer effortless back-up and recovery, and reduce our "IT footprint."

A third example of CDA's participation in a State level IT initiative is the State SharePoint and Office 365 Project (web-based alternative to shared drive). Many CHHSA departments already use SharePoint and have dedicated one or more full time positions to administer SharePoint servers. CDA does not have the resources or expertise to accomplish this on our own. CDA has a preliminary offer for IT staff support from

Analysis of Problem

California Department of State Hospitals to assist with the initial implementation; however, CDA will still lack the staff required for ongoing SharePoint administration.

A fourth example of CDA's participation in a State level IT initiative is ongoing contribution to the CHHSA Open Data Portal. This requires CDA to regularly make available in prescribed format our "publishable" data for access by the public via the central portal. IT staff need to be available to assist CDA with reviewing, selecting and preparing data and metadata in accessible formats for the public to understand, reuse and redistribute.

D. Justification

Staffing Comparison

At CDA, seven IT Branch staff provide the full range of IT services to 117 CDA staff. By comparison, the Department of Community Services & Development (CSD), a department comparable to CDA in size (107 staff) and IT requirements, has an IT shop of 15 PYs to address a very similar workload. The CSD IT branch includes a DPM III, a Business Analysis Team of 4 PY (1 Senior, 2 Staff and 1 Associate Information Systems Analyst), a Network Support team of 4 PY (2 Associate and 2 Assistant Information Systems Analyst), a dedicated ISO (Systems Software Specialist II), an application development staff of 4 PYs, and a supervisor (Data Processing Manager II) over the Network Support and Business Analysis teams.

At CSD a staff of 10 covers the responsibilities of ISO, supervision, Network Support and Business Analysis. CDA has only one full-time junior network support person and the CIO himself. (The CIO acts as ISO, supervisor, and Technology Recovery Coordinator. He also assists with the most difficult issues and performs the written analytical assignments in Unit, including state level reporting, business analysis, and administrative write ups.)

Growth in General IT Workload

Over the past decade, technological changes have steadily added to IT unit responsibilities, while at the same time budget reductions have reduced IT resources. The following is a partial list of tasks that have been added to workload with no commensurate increase in staffing:

- Monitoring threats (network intrusions, viruses, etc.)
- Conducting more expansive system and facility risk assessments
- Responding to increased oversight and accountability requirements for mandated reporting and mitigation tracking
- Responding to new standards for protecting, transmitting and using Personal Health Information PHI (PHI)
- Attending more outside meetings to keep up with technological and policy changes (State and CHHSA level CIO, ISO, TRP meetings.)
- Keeping pace with at least the minimally-required technological upgrades
- Sharing data and complying with data compatibility requirements; preparing, posting and updating publishable data the Open Data Portal
- Learning and implementing more sophisticated encryption technologies
- Purchasing, deploying and supporting a broader array of electronic equipment for employees (PDAs, mobile devices, Bring-Your-Own Devices)
- Deploying safe wireless technology
- Reviewing security related contractual terms-and-conditions for CDA's numerous local assistance and other contractors
- Participating in HIPAA audits and SLAA (formerly FISMA) reviews

Analysis of Problem

- Keeping up with increasing system and network complexity
- Addressing urgent security concerns requiring immediate actions such as patching, system monitoring, blocking IP addresses or establishing email rules to prevent active attacks

Impact of Limited Staffing on Network Stability

All of the added workload has resulted in having time to only address the most critical tasks, while more and more non-urgent tasks, such as maintenance, risk assessments, planning for disaster response, security upgrades and required reporting are delayed or neglected. The outcome is a gradual erosion of CDA's infrastructure and the integrity of the CDA's network and other systems. This exposes CDA to more risk and increases the amount of time spent putting out fires, implementing temporary fixes and responding to help desk tickets. The following partial list provides an idea of the types of issues impacting CDA's network as a result of limited staffing:

- Because network issue resolution requires rebooting servers after hours, CDA's one network person must be onsite both during business hours to address day-to-day operational issues and after hours and on weekends to resolve any network issues and reboot. This is hard to manage and requires the department to spend more for overtime pay.
- CDA does not have an up-to-date Technology Recovery Plan (TRP) and therefore cannot guarantee an effective response to disaster and system outages. CDA is not currently in compliance with SAM Sec. 5325.1 to plan for protection of critical information technology assets.
- CDA's Windows 2008 Domain Controller is failing and Microsoft Support is not able to determine issues or fixes. Microsoft Customer Support has recommended that CDA rebuild the Domain Controller with Windows 2012.
- Group Policies are corrupted and need to be reconfigured. Until that can be done, pushing out changes and managing permissions must be done manually and by exception. Because of this issue, when patching software is pushed out to fix security vulnerabilities and bugs it misses about 30% of computers on the network. Staff are required to manually apply critical updates.
- Use of old Access database technology in the CBAS Branch means that separate patches need to be deployed to all computers in that unit since Access is still using 32-bit technology. The rest of the department is upgraded to 64-bit.

An ongoing issue with the web filtering software prevents department staff from accessing websites (jobs.ca.gov, Agency SharePoint sites, etc.) they need to access in the commission of their duty. This requires manual intervention by the Help Desk each time it occurs.

Growth in Medi-Cal Related Workload

Over the past decade, the CBAS Branch has consumed much of the IT Branch's capacity for application development and maintenance. But currently they are relying on an outdated Access database application that is time-consuming to maintain and can no longer be modified to accept new data or functionality. On top of that, new needs for automation have arisen. The number of CBAS providers is anticipated to increase because both the State Settlement Agreement that guided the transition of CBAS to managed care and the State moratorium on new ADHC/CBAS licensees have expired. In addition, there are new federal requirements related to 1) the Affordable Care Act (ACA) Provider Enrollment Screening, 2) the CMS Home and Community-Based Settings (HCBS) Regulations, and 3) the updated 1115 Waiver. All of these developments will significantly increase the need for IT support in the Medi-Cal Branch.

To meet the above mandates, additional IT staff resources are needed to convert the existing inward facing database application from Access to SQL and to develop a new database module. The system needs to have an external interface that can be accessed by CDA staff in the field and also has the capacity to accept secure data transfer so that the mandated data analysis and reporting can finally be automated. Although CDA's IT Branch has qualified programmers, they do not have a person with the expertise needed to assist program staff with business, system, and security needs analyses. The project is expected to be within CDA's delegated authority but because the new requirements include collecting PHI, the system and supporting applications will need to be state-of-the-art with sophisticated security and encryption capability.

Analysis of Problem

The MSSP Branch is in a similar situation. Their database application does not provide them with reliable automated data validation, error identification and correction. Staff need the ability to access site information from the field and to securely collect, report, and maintain data to meet federal waiver requirements.

Below is a brief description of the personnel and expertise the department needs to meet minimum State IT requirements and to properly address CDA's existing infrastructure weakness and database issues.

Position Workload Summary (See attached for workload detail.)

1. Information Security Officer/Technology Recovery - 1.0 Data Processing Manager I

Per SIMM 5305-A, each State entity is to have an Information Security Officer (ISO). With limited staff and resources, CDA has historically combined this role with the CIO position. Likewise, there is requirement for a Technology Recovery Coordinator; again due to a lack of resources the CIO has historically filled this role as well.

Since CDA does not have positions or adequate expenditure authority to be able to augment IT staffing, the CIO necessarily takes on both the ISO and Technology Recovery Coordinator duties as well. Because there are limited staff positions, this individual also takes on other critical responsibilities that are more appropriately staff-level duties. So when tasks are prioritized, the urgency of daily operations many times takes precedence over important tasks such as risk assessments and disaster recovery preparations. The result is an ever growing list of important tasks that do not get the attention they desperately deserve. Additionally, State standards are that the ISO be an independent and separate function to provide checks and balances and maintain objectivity related to security issues and reporting.

In December of 2013, the California Department of Military provided CDA a free risk assessment as part of their pilot program to provide this service to State departments. The assessment did not reveal any highly critical risk; however, dozens of other potential vulnerabilities were identified that have yet to be addressed.

Not having a person dedicated to disaster planning, testing and recovery has resulted in CDA falling behind in this area as well. The Department's Technology Recovery Plan is outdated and our backup for critical IT functions has not been tested recently, which is unacceptable. In addition, CDA plans to replace our old backup system with a more modern and easy to maintain cloud-based solution. But, a staff person is needed to analyze, plan, and implement that alternative.

The ISO / Technology Recovery position's duties will include the following:

- Vulnerability assessment and risk mitigation related to servers, networks and applications
- Physical security measures for the building, network, ports, and equipment
- Threat detection, actively monitoring for network intrusion, viruses, malware
- Provide security training and alerts for staff
- Participate in Agency and State level ISO meetings, forums and training
- Technology Recovery Coordinator
- Plan, test and implement weekly and monthly back-up procedures
- Create, test and maintain a functioning Technology Recovery Plan
- Represent the department in disaster recovery exercises
- Participate in Agency and State level Technology Recovery Coordinator meetings, forums, training, surveys, and committees

2. Network Administrator - 1.0 Staff Information Systems Analyst

The most critical position in IT is the network administrator. The network administrator plans, builds and most importantly keeps the network up and running so the rest of the department has access to computer related resources required in performing their duties.

Analysis of Problem

In August of 2013, the Department of Aging suddenly and unexpectedly lost their network administrator. The Help Desk Coordinator stepped in to assume a network support role with the hope that individual could eventually assume the full range of duties. However, the CIO has since realized that a more experienced and highly trained expert is needed to address the more complex issues, stabilize the existing network infrastructure and lead the effort to plan for and transition the Department's network infrastructure to another CHHS department to take advantage of economies of scale. In addition, this position is needed to help with the migration of servers and applications to the Cloud and the implementation of the State's SharePoint initiative.

The Network Administrator position's duties will include the following:

- Shore up and maintain the network; build, configure, install and maintain network devices such as servers, domain controllers, routers, and switches
- Design and implement network architecture to meet department needs; trouble shoot and respond to unanticipated emergencies
- Install critical patch and firmware updates to servers, desktop and laptop computers on a weekly basis
- Administer email servers and services
- Plan and coordinate the department's migration of servers and applications to Cloud services Administer internal and external website servers
- Plan and coordinate the migration of network infrastructure to a confederated service agreement within CHHS Agency
- Oversee and coordinate the department's implementation of the State's SharePoint initiative

3. IT Systems, Project and Reporting Analyst - 1.0 Staff Information Systems Analyst

CDA does not have a position or IT staff with the expertise to work with program staff to gather business and technical needs, analyze and document technical program requirements, serve as a project manager or perform all of the statewide reporting requirements. Along with an ongoing need for this type of expertise, the Department has a critical need for expertise to assist with the updating the MSSP and CBAS program applications and incorporating the recent federal ACA and Medi-Cal data collection and reporting requirements.

The department has several production applications in Access databases that will need to be replaced prior to moving them into the Cloud.

The Project and Reporting Analyst position's duties will include the following:

- Analyze MSSP Medi-Cal requirements and serve as project manager overseeing the incorporate the requirements into the application
- Analyze CBAS Medi-Cal requirements and serve as project manager overseeing the incorporate the requirements into the application
- Analyze and find alternatives for existing applications in Access databases
- Assist in the risk assessments
- Participate in the development and writing of Technology Recovery Plan
- Serve as the Open Data Portal project IT data coordinator and data management coordination, including preparing directory of data assets and libraries of business analysis artifacts, documents,data and metadata standards and data reporting methods.
- Project manager

Analysis of Problem

4. Upgrade CIO Chief Information Officer Upgrade (to DPM III)

The CIO position for the Department of Aging needs to be a higher classification that is consistent with the full range of responsibilities, required level of expertise and strong leadership skills needed to fulfill the requirements of the CIO position. There are no subordinate supervisors in the Unit, and, therefore, one position covers all the duties of a regular CIO and performs all the daily operational management and supervision, along with directly overseeing, troubleshooting and performing the higher level functions in the Office. This one position is also responsible for project management and for preparing and submitting all of the required state level annual planning documents and reports. Individuals that possess the required broad experience, higher level of expertise and willingness to take on the exorbitant workload associated with this unique position are rarely available within the State DPM II candidate pool. This upgrade is supported from an HR allocation perspective, is consistent with the CIO level in other smaller departments and has strong support from the CHHSA AIO.

E. **Outcomes and Accountability**

The increased staffing level from the approval of this BCP will enable CDA to address many critical departmental IT needs. It provides the resources to stabilize, update and manage our failing network infrastructure and perform on going risk assessment and threat monitoring improving the security of our network and HIPAA data. The staffing level also allows for the analysis of program needs and the conversion of those business needs into IT requirements that will permit the program to meet new data collection and reporting mandates. There will be adequate staff available to establish a more complete and tested back-up system that will serve as foundation for a Technology Recovery Plan to be in compliance for the first time since 2010.

Projected Outcomes

Workload Measure	CY 2015-16	BY 2016-17	BY+1 2017-18	BY+2 2018-19	BY+3 2019-20	BY+4 2020-21
PC Patch Schedule dedicated hours	12	39	52	52	52	52
Threat Monitoring dedicated hours	12	180	240	240	240	240
Department Computers Encryption percentage	34%	70%	85%	100%	100%	100%
Technology Recovery Planning and backup percentage completed	35%	50%	90%	100%	100%	100%

F. **Analysis of All Feasible Alternatives**

Alternative 1: Approve the Request. This BCP seeks the PY and expenditure authority necessary to meet minimal State level requirements for IT. It is a resource-efficient plan that takes into account the ability to leverage existing resources of CHHS Agency sister departments. This alternative will ensure the department's full compliance with HIPAA and state security and will allow the Department to come into compliance with federal Medi-Cal requirements.

Alternative 2: Do nothing. Medi-Cal PHI may be subject to risk. Not being able to respond to Medi-Cal changes and requirements puts the Department's Interagency Agreement with DHCS to administer MSSP and CBAS at risk and in general jeopardizes the Department's ability to support our network and meet

Analysis of Problem

State security requirements. This alternative would require the Department to seek exemption to retain an expensive outside consultant who can be available for network failure emergencies and can assist with the more complex issues.

Alternative 3: Attempt to retain temporary help with the necessary expertise to fulfil these IT functions. Obtaining expertise on an as needed basis is time consuming, with no guarantee of finding the necessary expertise. Often there is a steep learning curve as individuals familiarize themselves CDA operations. In addition, this alternative does not provide for long term stable expertise and the Department would still need additional expenditure authority for this temporary assistance.

G. Implementation Plan

Two positions effective July 1, 2016. CDA plans to seek current authority for one position to address critical situations and bridge the gap between now and July 1. In the meantime, the Department will need to prevail upon sister departments and utilize temporary help for assistance; and, to the extent possible, CDA will recruit permanent staff in advance and be ready to hire on July 1, 2016.

H. Supplemental Information (See workload attachments)

I. Recommendation

Approve Alternative 1. This is the best solution because it not only provides on-site staffing to meet minimum security and other requirements, but also take into account any opportunity to leverage existing resources and the economies of scale offered by partnering with CHHS Agency sister departments.

1.0 Program Analyst
(Limited Term Staff: July 1, 2016 - June 30, 2018)
Workload Analysis

CDA - Information Technology Unit	Hours
Best Practices Development and Implementation	
Collaborate with ISO and ITB Team to develop departmental best business practices and technical requirements	156
Develop Data Flow diagrams of new and modified software	156
Data management: Assist Data Team with Open Data projects. Prepare directory of data assets, library of business analysis artifacts, documents, metadata, data standards and data reporting methods.	102
Department Liaison	
Prepare justification or solicitation documents to acquire external service contractors/consultants to facilitate the development and/or enhancement of CSD's systems	52
Assist, support, and train staff on use of the system functions and transactions.	26
Department IT Evaluation and Analysis	
Department liaison with end-users and other units to develop efficient and optimal workflow processes and application systems	208
Assist external customers in performing user requirement traceability to validate software functionality and deliverables to meet documented business/program requirements	52
Work with peers in the Information Technology Services Unit to review and establish appropriate IT policies and procedures. Gathers and shares higher level view of systems to assist in design of Enterprise Architecture.	52
Reporting	
Prepare formal System Requirement Reports, Feasibility Study Reports (FSR), Special Project Reports (SPR), and Post Implementation Evaluation Reports (PIER).	140
Prepare and analyze monthly reports of IT issues for unit meetings	104
IT Analysis	
Analyze and document business system requirements for all application development, including but not limited to use case documentation, functional requirements, test scripts and/or training materials by need of the department	52
Analyze suitable "build or buy" business systems and provide direction for maximum return on investments to meet departmental needs.	52
Monitor progress of the software development lifecycle associated to service requests, prepare user documentation and/or update user guides for any projects.	52
Review technical documentation and discover emerging technologies and methodologies to educate Information Technology Business Unit team members and management.	52
Identify business requirements and resolves application related questions for the incumbent's assigned projects.	52
Analyze the long term cost and ROI to make recommendations for Build or Buy decisions	52
Review CHHS Agency application portfolio for existing software that can be leveraged rather than recreated	24

Conduct research to clarify or add details that developers may have about a service requests and performs analysis to recommend the best alternative to resolve project issues.

Internal Project Management	
Project Manager for complex IT projects, develop schedules, establish document libraries, oversee project details to ensure project is completed on within scope	156
Assist ISO in the risk management and technology recovery analysis, Technology Recovery Plan documentation	184
Total Hours	1,776
PY	1.00

**1.0 Information Security Officer
(Permanent Staff July 1, 2016 - On-going)
Workload Analysis**

CDA - Information Technology Unit	Hours
Vulnerability and Threat Management	
Network, Application, website scanning and vulnerability identification.	120
Critical enterprise patch deployment on department wide workstations and servers to reduce surface-level attacks and server vulnerabilities via server hardening.	48
System monitoring and log updates regarding third party threats, employee policy violations, other system risks with detection software.	72
Department wide Symantec Full Disk AES Encryption implementation and monthly security maintenance	532
System log review and analysis of security incident and failed access reports.	160
Assist Network Administer with forensic analysis of security or system breaches, employee policy violations and other security related incidents.	120
Data Loss Prevention	
Collect and review Departmental Data Release Forms to secure avenues for external data tracking and transfers	21
Collect and review Departmental USB Access Control Forms	5
Application Security	
Sets roll based access controls in secure applications to limit contracts and internal developers' to set job roles using N-Tier Architecture.	60
Risk and Change Management	
Develop and maintain the NIST-based risk assessments. Perform ongoing compliance assessments of business partners, to measure compliance with agreements. Performs bi-annual risk assessments with third party vendors.	228
Authorize change to control firewall ports openings and other processes. Assess possible changes to the published enterprise IT standards with a formal committee.	3
Governance	
Manage information security policies and ensures all employees adhere to the guidelines in place.	16
Establish and enforce hardware and software standards	8
Disaster Recover Planning	
Establish, maintain, and test the Technology Recovery Plan in accordance with CHHS and SIMM requirements.	120
Training, Meetings and Formal Documentation	
Contribute and edit content for Privacy and Security in-person and online training.	84
Departmental Liaison - attend and participate State and Agency level meetings to give feedback and CDA analysis as needed.	216
Annual reporting when needed	6

Medi-Cal Program - MSSP/CBAS	
HIPAA Compliance	
Review and inspect Websense system traffic to prevent inappropriate transfer of sensitive data such as social security numbers and HIPPA recipient information	16
Analyze interagency HIPAA agreements and coordinate with HIPAA Compliance Officer for security compliance.	36
Governance	
Co-write and implement HIPAA policy updates.	16
Manage information security policies and ensures all employees adhere to the guidelines in place.	12
Total Hours	1,899
PY	1.07

1.0 Network Administrator
(Permanent Staff July 1, 2016 - On-going)
Workload Analysis

CDA - Information Technology Unit	Hours
Hardware Maintenance	
Build, configure, and upgrade network devices to department wide servers, domain controllers, routers, printers and switches.	180
Maintain the server racks and room.	24
Network Creation and Maintenance	
Design, establish and monitor department's network including over 120 PC's 40 laptops and 12 servers.	96
Develop implement policies for directory structures, naming conventions, active directory and group policies.	156
Create and maintain Virtual Private networks for remote access.	48
Server and Device Patch Management	
Maintain inventory of all shared drive devices on the network and ensure all devices are patched weekly, and anytime critical alerts are issued.	240
Security Management	
Provide appropriate encryption solution for servers, laptops and desktop PC.	196
Administer weekly back-ups, send back-ups off site, recall back up tapes for department restoration.	156
Assist investigations by saving and analyzing files and directories. Incorporate and administer firewalls.	220
Mobile Devices	
Establish and maintain Departmental cell phone policies	5
Cell phone security - tracking and remote deletion of cell phone content	5
Customer cell phone support	5
Email Administration	
Add, delete and update user accounts	52
Establish and maintain filters for content, spam, viruses and other threats	26
Other IT Administrative Needs	
Establish and administer additional services such as FTP, List Serves, SharePoint, web servers and content filters.	408
Provide user support in establishing and deleting accounts.	52
Total Hours	1,869
PY	1.05

Personal Services Details

		Salary Information								
Positions		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>
1312	- Staff Info Sys Analyst (Spec) (Eff. 07-01-2016)				0.0	2.0	2.0	2.0	2.0	2.0
1381	- Dp Mgr I (Eff. 07-01-2016)				0.0	1.0	1.0	1.0	1.0	1.0
Total Positions					0.0	3.0	3.0	3.0	3.0	3.0