

STANDARD AGREEMENT
FOR I.T. GOODS/SERVICES ONLY

	REGISTRATION NUMBER
PURCHASING AUTHORITY NUMBER	AGREEMENT NUMBER
CDT-7502	16-10645

1. This Agreement is entered into between the State Agency and the Contractor named below
STATE AGENCY'S NAME
California Department of Technology, hereinafter referred to as the "CDT" or the "State"
CONTRACTOR'S NAME
Grant Thornton, LLP, hereinafter referred to as the "Contractor"

2. The term of this Agreement is: July 15, 2016 (or upon approval, whichever is later), through July 14, 2017

3. The maximum amount of this Agreement is: \$ 1,500,000.00 (One Million Five Hundred Thousand Dollars and Zero Cents)

4. The parties agree to comply with the terms and conditions of the following attachments which are by this reference made a part of the Agreement:

Exhibit A – Statement of Work	Page 2-9
Exhibit A-1 – Staff Resources Resumes	Page 10-17
Exhibit A-2 – Work Authorization	Page 18-20
Exhibit A-3 – Personnel Change Order Request Form	Page 21
Exhibit A-4 – Work Authorization Acceptance Document	Page 22
Exhibit B – Budget Detail and Payment Provisions	Page 23
Exhibit B-1 – Cost Worksheet	Page 24
Exhibit D – Special Terms and Conditions to Safeguard Federal Tax Information	Page 25-29
Exhibit E – Security and Data Protection	Page 30

RFO #15-2052534-A, Contractor's Response and MSA Contract #5137002-119 are here by incorporated by reference as if attached hereto.
 (California Department of Technology Info Only: WO# 2052534)

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.

CONTRACTOR	California Department of General Services Use Only
<small>CONTRACTOR'S NAME (If other than an individual, state whether a corporation, partnership, etc.)</small> Grant Thornton, LLP	
<small>BY (Authorized Signature)</small> 	<small>DATE SIGNED</small> 7/13/16
<small>PRINTED NAME AND TITLE OF PERSON SIGNING</small> Graeme Finley, Managing Director	
<small>ADDRESS</small> 770 L Street, Suite. 950, Sacramento, CA 95814	
STATE OF CALIFORNIA	
<small>AGENCY NAME</small> California Department of Technology	
<small>BY (Authorized Signature)</small> 	<small>DATE SIGNED</small> 7/13/16
<small>PRINTED NAME AND TITLE OF PERSON SIGNING</small> Jennifer Herrera, Purchasing Manager	
<small>ADDRESS</small> P.O. Box 1810 MS Y-18 Rancho Cordova, CA 95670	
<input type="checkbox"/> Exempt	

EXHIBIT A
STATEMENT OF WORK

1. OBJECTIVE

The pace of technological change presents significant opportunities for CDT/OTech, including an increased potential for innovation and transformation. This also presents risk to the CDT/OTech's service and financial structure that must be identified and addressed prior to the implementation of change. In order for CDT/OTech to improve agility and be better positioned to keep pace with industry changes, CDT/OTech seeks to partner with a qualified contractor to:

- Review current chargeback structure;
- Identify service delivery opportunities;
- Optimize rates;
- Determine opportunities to align services with customer demand; and,
- Identify the business and financial impact of service-related changes.

2. TERM/PERIOD OF PERFORMANCE

- a. The period of performance for the Contract shall be from July 15, 2016, or upon approval, whichever occurs later, through July 14, 2017, with the option to extend for one (1) additional 12 month term at the original rates evaluated and considered and executed at the State's sole option.
- b. The Contractor shall not be authorized to deliver or commence the performance of services as described in this Statement of Work (SOW) until written approval has been obtained from all entities. Any delivery or performance of service that is commenced prior to the signing of the Contract shall be considered voluntary on the part of the Contractor and non-compensable.
- c. Consistent with the terms and conditions of the original solicitation, and upon mutual consent, CDT/OTech and the Contractor may execute written amendments for changes to this Contract that were evaluated and considered.

3. QUALIFICATIONS

CDT/OTech is seeking a Contractor with demonstrated experience analyzing technical services and rate structures for IT service providers with a diverse portfolio of service offerings. The Contractor will be expected to provide documentation, including staff references to validate their experience. The Scope Definition, defined in the Work Authorization (WA), will aid the Contractor in determining the skills needed for each WA engagement. The Contractor shall propose the classification type and number of personnel needed for each engagement. Contractor staff **MUST** meet the Mandatory Qualifications in order to be considered for evaluation. Interviews are not a part of the evaluation and selection process; however, they may be conducted at the discretion of CDT/OTech

a. Mandatory Qualifications**3.1 Contractor Company Qualifications**

The Company is required to meet the following minimum qualifications, which must have occurred within the past five (5) years:

- At least four (4) years of experience performing cost/benefit analysis, that includes identifying total cost of ownership, IT service rate development, and return-on-investment. This experience must relate to previous engagements with IT service providers.
- At least three (3) years of experience evaluating current lines of business for IT organizations and providing recommendations, or a roadmap, for future lines of business and changes to current lines of business.
- At least three (3) years of experience providing organizational change management assessment and recommendations.

3.2 Contractor Staff Qualifications

The Contractor must provide qualified staff who collectively meet the qualifications described below in addition to the education and experience required for each awarded in the IT Consulting Master Service Agreement (MSA). Staff experience worksheet and resumes must show relevant experience. The proposed classification must be allowed in the Contractor's IT Consulting MSA contract.

Any combination of the following awarded classifications, as allowed in the Contractor's individual IT Consulting MSA may be offered:

- Senior Project Manager
- Project Manager
- Senior Technical Lead
- Technical Lead
- Systems Analyst

Additional required experience includes a minimum of five (5) years conducting financial analysis of IT service providers. Experience must include extensive knowledge of:

- Governmental cost accounting
- Cost benefit analysis
- Calculating total cost of ownership
- Calculating return on investment
- Developing IT service rates
- Developing IT service rate methodologies
- Financial Analysis
- Business analysis for government clients
- Developing IT roadmaps

The Contractor is responsible for notifying the Contract Administrator if there is a substitution or addition of consultant staff for any reason. See number 7.d of the SOW.

b. Desirable Qualifications

It is desirable that Contractor staff meet the following qualifications and possess certifications in the technologies listed below.

- At least four (4) years' experience of mainframe, Windows, Linux, and AIX platforms.

- Knowledge of major CDT program areas.

4. PROJECT TASKS AND PROJECT DELIVERABLES

The Contractor will review existing services and associated financial models and recommend service-related changes. Specific areas of focus may include, but not limited to:

- Review the current rate methodology used by CDT to recover costs for specific services and make improvement recommendations on how that methodology can be improved and streamlined
- Analyze technology tools used by CDT/OTech and make recommendations on how costs can be reduced, which tools can be eliminated, added, etc.
- Recommend new service opportunities for OTech

CDT/OTech will work closely with the contractor to finalize the deliverables and to agree on the specific tasks to be performed. Work Authorization forms will be used to document and authorize the specific tasks and deliverables and allocated timeframes and costs.

Contractor provided recommendations must specify opportunities for service enhancements, consolidation, discontinuation and/or contractor provided and hosted services. The recommendations must include sufficient financial detail to guide decisions and support financial stability. CDT/OTech anticipates the execution of contractor recommendations will be performed by CDT/OTech. Services to be reviewed may be comprised of one or more of the following components:

- Platform (Windows, Unix-based, and Mainframe)
- Storage (SAN, NAS, backup and restore)
- Software services (databases, middleware, web servers, etc.)
- Network components (firewalls, proxy, DNS, etc.),
- Service management and monitoring tools

Business Objectives

An assessment of CDT/OTech's current service structure, including hardware, software, costs and resources, and recommendations for changes to the service structure that will enhance service delivery and maintain or improve financial stability.

a. Project Tasks and Deliverables

CDT/OTech will partner with the selected contractor to identify service areas to be reviewed. Specific review requirements and outcomes will be identified and documented on Work Authorization forms prior to the commencement of work. The outcomes may include:

- Recommendations for hardware and software changes to enhance services
- Financial models that identify rate adjustments required for cost recovery, as well as potential new rate development methodologies
- Recommendations for new service opportunities that would benefit CDT/OTech customers
- Resource levels required for service-related changes
- Recommendations on organizational change management frameworks to guide the CDT/OTech transformation into a next generation IT service provider

5. ACCEPTANCE OF TASKS AND DELIVERABLES

It shall be in the State's sole determination as to whether a project task/deliverable identified in this Contract or in a supplemental Work Authorization (WA), Exhibit A-2 has been successfully completed and acceptable to the State. Acceptance criteria shall consist of the following:

- a. The approval process is outlined in Section 10 – Performance.
- b. A signed WA Acceptance Document (WAAD), Exhibit A-4 is required for each project task/deliverable identified in a WA.
- c. The Contractor shall meet all time-lines, as agreed to in the Contract or in WA.

6. CONTRACTOR REPORTING REQUIREMENTS

The Contractor will submit weekly written status reports in MS Word format to the CDT/OTech Contract Administrator as directed. The reports shall be detailed regarding current status and future activities. Status reports are required weekly but are **not** considered deliverables under the terms of this Contract. These reports shall include, but are not limited to:

- a. A summary of the work completed during the reporting period, showing actual vs. planned.
- b. Highlighted tasks that are behind schedule, remediation plans, and overall impact on the project.
- c. The status of the overall engagement and all categories of requested services, including discussion of risks, problems encountered, solutions, and proposed solutions.
- d. The tasks expected to be completed in the next reporting period.
- e. An accounting of Contractor staff person(s) hours for the prior week and for the Contract to date i.e. time sheets.
- f. Ad hoc reporting as required.
- g. If requested, the Contractor shall participate in periodic briefings for Executive Management, as deemed appropriate by CDT/OTech.

7. CONTRACTOR RESPONSIBILITIES

- a. The Contractor will provide its own equipment necessary to perform the required duties.
- b. The Contractor shall designate a primary contact person to whom all project communications may be addressed and who has the authority to act on all aspects of the services.
- c. The Contractor will notify CDT/OTech, in writing, of any changes in the personnel assigned to the tasks. If a Contractor employee is unable to perform due to illness, resignation, or other factors beyond the Contractor's control, the Contractor will make every reasonable effort to provide suitable substitute personnel. The substitute personnel must be equal or better qualifications than the replaced personnel and must be approved in advance of any performance under the Contract by the CDT/OTech Contract Administrator via an approved Personnel Change Order Request/Authorization form, Exhibit A-3 with attached resume and must provide history of their particular

relevant experience. The rates for the substituted personnel must be less than or equal to the rates of the personnel that they are replacing.

- d. The Contractor personnel shall perform their duties on any of the premises of the CDT/OTech facilities located within the greater Sacramento area during regular State business hours, and at all other times as required to successfully provide the services described in this SOW.
- e. The Contractor will adhere to CDT/OTech policies and procedures, including access and security requirements.

8. DEPARTMENT OF TECHNOLOGY RESPONSIBILITIES

- a. Designate a person to whom all Contractor communication may be addressed, and who has the authority to act on all aspects of the services. This person will review the SOW and associated documents with the Contractor to ensure understanding of the responsibilities of both parties.
- b. Provide Contractor personnel with standard Department imaged desktop(s), phone equipment, and standard cubicle and/or office working facilities at any of the CDT/OTech sites and/or other locations specified by the CDT/OTech, as necessary, with appropriate network connectivity to access team working documents.
- c. Provide access to Department staff and management, offices and operation areas, as required, to complete the tasks and activities defined under this Contract.
- d. Provide at least a minimum of ten (10) State business days for the timely review and approval of information and documentation provided by the Contractor to perform its obligations.
- e. Provide information regarding the business structure of the CDT/OTech, and schedule the availability of the CDT/OTech personnel for interviews, as required by the Contractor.
- f. The Contractor personnel shall perform their duties on any of the premises of the CDT facilities located within the greater Sacramento area during regular State business hours, and at all other times as required to successfully provide the services described in this SOW. The Contractor and the State may mutually agree to allow a portion of the time and/or work be completed remotely, at a location determined by the Contractor. When/If working remotely, the Contractor personnel staff must adhere to the CDT Telework Policies and Procedures (number 2017) and the Remote Access Request Procedure (number 3134).

9. WORK AUTHORIZATIONS

- a. Each WA shall consist of a detailed statement of the purpose, objective, or goals to be undertaken by the Contractor and all information requested to be provided per WA form, Exhibit A-2.
- b. All WA must be in writing prior to beginning work and signed by the Contractor and the CDT/OTech Contract Administrator.
- c. The CDT/OTech has the right to require the Contractor to stop or suspend work on any WA.

- d. Personnel resources will not be expended (at a cost to the CDT/OTech) on task/deliverable accomplishment in excess of estimated work hours required unless the procedure below is followed:
- 1) If, in performance of the work, the Contractor determines that a WA to be performed under this Contract cannot be accomplished within the estimated work hours, the Contractor will immediately notify the CDT/OTech in writing of the Contractor's estimate of the work hours which will be required to complete the WA in full. Upon receipt of such notification, the CDT/OTech may:
 - (a) Authorize the Contractor to expend the estimated additional work hours or service in excess of the original estimate necessary to accomplish the WA;
 - (b) Terminate the WA; or
 - (c) Alter the scope of the WA in order to define tasks that can be accomplished within the remaining estimated work hours.
 - 2) The CDT/OTech will notify the Contractor in writing of its decision within seven (7) calendar days after receipt of the notification. If notice of the decision is given to proceed via an amended WA signed by the Contractor and CDT/OTECH, the Contractor may expend the estimated additional work hours for agreed upon services. The CDT/OTech agrees to reimburse the Contractor for such additional work hours.

10. PERFORMANCE

The CDT/OTech will be the sole judge of the acceptability of all work performed and all work products produced by the Contractor as a result of this SOW. Should the work performed or the products produced by the Contractor fail to meet the CDT/OTech conditions, requirements, specifications, guidelines, or other applicable standards, the following resolution process will be employed, except as superseded by other binding processes:

- a. The CDT/OTech will notify the Contractor in writing within five (5) State business days after completion of each phase of service of any acceptance problems by identifying the specific inadequacies and/or failures in the services performed and/or the products produced by the Contractor.
- b. The Contractor will, within five (5) State business days after initial problem notification, respond to the CDT/OTech by submitting a detailed explanation describing precisely how the identified services and/or products actually adhere to and satisfy all applicable requirements, and/or a proposed corrective action plan to address the specific inadequacies and/or failures in the identified services and/or products. Failure by the Contractor to respond to the CDT/OTech's initial problem notification within the required time limits may result in immediate termination of the Contract. In the event of such termination, the CDT/OTech shall pay all amounts due the Contractor for all work accepted prior to termination.
- c. The CDT/OTech will, within five (5) State business days after receipt of the Contractor's detailed explanation and/or proposed corrective action plan, notify the Contractor in writing whether it accepts or rejects the explanation and/or plan. If the CDT/OTech rejects the explanation and/or plan, the Contractor will submit a revised corrective action plan within three (3) State business days of notification of rejection. Failure by the Contractor to respond to the CDT/OTech's notification of rejection by submitting a revised corrective action plan within the required time limits may result in immediate

termination of the Contract. In the event of such termination, the CDT/OTech shall pay all amounts due the Contractor for all work accepted prior to termination.

- d. The CDT/OTech will, within three (3) State business days of receipt of the revised corrective action plan, notify the Contractor in writing whether it accepts or rejects the revised corrective action plan proposed by the Contractor. Rejection of the revised corrective action plan will result in immediate termination of the Contract. In the event of such termination, the CDT/OTech shall pay all amounts due the Contractor for all work accepted prior to termination.

11. PROBLEM ESCALATION

The parties acknowledge and agree that certain technical and project related problems or issues may arise, and that such matters shall be brought to the CDT/OTech's attention. Problems or issues shall normally be reported in regular status reports. There may be instances, however, where the severity of the problems justifies escalated reporting. To this extent, the Contractor will determine the level of severity and notify the appropriate CDT/OTech personnel. The CDT/OTech personnel notified, and the time period taken to report the problem or issue, shall be at a level commensurate with the severity of the problem or issue. The CDT/OTech personnel include, but are not limited to, the following:

- | | |
|---------------|--|
| First level: | Project Director |
| Second level: | Assistant Chief, Office of Technology Services |
| Third level: | Chief, Office of Technology Services |

12. CANCELLATION

The CDT/OTech may exercise its option to terminate the Contract at any time with 30 calendar days prior written notice. In the event of such termination, the CDT/OTech shall pay all amounts due the Contractor for all deliverables accepted prior to termination.

13. OTHER CONTRACT CONSIDERATIONS

- a. The Contractor will act as prime contractor under this Contract. In addition to identifying all personnel proposed to work under this Contract, the Contractor shall also identify its subcontractor affiliation, as applicable.
- b. The CDT/OTech reserves the right to approve all subcontractors prior to the performance of any work by the subcontractor.
- c. Nothing contained in this Contract shall create any conceptual relationship between the State and any subcontractors, and no subcontract shall relieve the Contractor of its responsibilities and obligations hereunder. The Contractor is fully responsible to the CDT/OTech for the acts and omissions of its subcontractors and of persons either directly or indirectly employed by any of them.
- d. If a subcontractor is a California Certified Small Business (SB) and/or Disabled Veteran Business Enterprise (DVBE), then those amounts paid to certified subcontractors shall be identified on the Contractor's invoice(s).
- e. The Contractor's obligation to pay its subcontractors is an independent obligation from the State's obligation to make payments to the Contractor. As a result, the State shall have no obligation to pay or to enforce the payment of any monies to any subcontractor.

- f. Military and Veteran Code (MVC) 999.5(d), Government Code (GC) 14841, and California Code of Regulations (CCR) 1896.78(e) requires all Prime Contractor’s that had a DVBE firm preform any element of work for a contract to report DVBE information.

Prime Contractors are required to maintain records supporting the information that all payments to DVBE subcontractor(s) were made. The Prime DVBE Subcontracting form can be found at the following link: <http://www.documents.dgs.ca.gov/pd/smallbus/Prime%20DVBE%20Sub%20Report.xls> and the instructions can be found at the following link: <http://www.documents.dgs.ca.gov/pd/smallbus/Prime%20DVBE%20Sub%20Report%20Instruction.doc>. Completed forms are to be e-mailed to: primeDVBE@state.ca.gov.

14. CONTRACT REPRESENTATIVES

All notices required by, or relating to, this Contract shall be in writing and shall be sent to the parties of the Contract at the address set below unless changed from time to time, in which event each party shall so notify the other in writing, and all such notices shall be deemed duly given if deposited, postage prepaid, in the United States mail or e-mailed and directed to the addresses then prevailing.

The contract administrators during the term of this contract will be:

State: California Department of Technology Name: Debra Gonzales Phone: 916-228-6166 e-mail: debra.gonzales@state.ca.gov	Contractor: Grant Thornton, LLP Name: Graeme Finley Phone: 571-242-0478 e-mail: Graeme.finley@us.gt.com
State: California Department of Technology Name: Ellen Ishimoto Phone: 916-228-6512 e-mail: Ellen.Ishimoto@state.ca.gov	

Direct all contract inquiries to:

State: California Department of Technology Unit: Acquisition & IT Program Management Branch Name: Theresa Jones Address: P.O. Box 1810 MS Y-18 Rancho Cordova, CA 95741 Phone: 916-431-4085 e-mail: Theresa.Jones@state.ca.gov	Contractor: Grant Thornton, LLP Name: Virginia Dawson Address: 770 L Street, Suite 950 Sacramento, CA 95814 Phone: 512-692-1235 e-mail: Virginia.dawson@us.gt.com
--	---

EXHIBIT A-1
STAFF RESOURCE RESUMES

The following 7 pages are Staff Resource Resumes.

Wei Tang, PMP, SMC, ITIL

Why Selected for this Role?

- Mr. Tang is a Certified Project Management Professional (PMP) and a Certified Scrum Master (SMC) who is also knowledgeable of ITIL principles.
- Mr. Tang leads the IT Strategy and Governance practice at Grant Thornton and has managed large IT finance, shared services and performance management projects for public and private sectors clients, ranging in size from \$40 million to \$4 billion.
- He assists clients to in achieving their business goals by defining strategies, formulating portfolios, prioritizing IT investments, justifying budget and allocating resources.
- He has implemented governance structures, cost models, processes and tools for his clients to improve efficiency.
- Mr. Tang has developed business case analysis and software development methodology such as waterfall and agile to assist clients with investment and management decisions.
- He has also implemented management processes and tools such as Oracle PPM and CA Clarity to evaluate and track IT budget, programs and procurements for his clients.

Relevant Experience

Department of Housing and Urban Development (HUD) – Implemented HUD’s New Core Interface Solution (NCIS) to support HUD’s migration of its core accounting and administrative functions to the Department of Treasury’s Administrative Resource Center (ARC)'s shared service environment. NCIS was the most critical element of this shared service solution because it enabled HUD and ARC to transfer and reconcile financial data between ARC’s Oracle Federal Financials and HUD’s legacy systems. This project was high priority for HUD, Treasury and Office of Management and Budget (OMB) because HUD was the first cabinet-level department shared service migration in the federal government. Managed project planning, execution and status reporting to the senior executives including HUD’s CFO, CIO and ARC’s Administrator.

Federal Motor Carrier Safety Administration (FMCSA) – Conducted an analytical framework called the Performance Driver Model™ (PDM) to assess FMCSA’s IT modernization program and IT investment practices. The assessment was directed by OMB after TechStat reviews. Conducted stakeholder interviews including business executives and regional service centers and offices, and collected and reviewed artifacts to assess the program. Developed a remediation plan to align with FMCSA’s performance goals, restructure the investment portfolios, strengthen IT governance processes, and deliver IT functionality using Agile methodology. Presented the findings and the plan to the agency’s Administrator and senior executives. OMB approved the funding for the modernization portfolio based on the new plan.

Department of the Interior (DOI) – Assisted the DOI Office of Chief Information Officer (OCIO) in developing and executing its portfolio management process for managing \$1 billion IT portfolio. Implemented a selection process which enables the department to evaluate, prioritize and select IT investments. Collaborated with management functions such as bureau CIOs, enterprise architecture, strategic planning and project management to formulate the department’s IT portfolio. Advised investment owners and project managers in developing their business cases. Analyzed the DOI portfolio structure and developed strategies for reducing the annual IT infrastructure cost. Improved the department’s IT

investments process by implementing a prioritization methodology. Responded to OMB's data calls and TechStat preparations. Assisted OCIO in administering the portfolio management toolset including eCPIC, SharePoint and Expert Choice.

Virginia Information Technology Agency (VITA) – Managed Commonwealth Technology Portfolio (CTP) implementation for the Commonwealth of Virginia. Led the engagement team to perform assessments, design and implement processes, develop system, conduct training, support operation and maintenance. The Commonwealth IT Investment Board (ITIB) used the solution to initiate, prioritize, manage and evaluate \$1 billion of IT investments including projects, applications, and infrastructure. The solution increased transparency and collaboration of the Commonwealth's IT budget process.

Bureau of Land Management (BLM) – Restructured the IT organization for BLM's Chief Information Officer to reduce annual spending from \$176 million to \$148 million. Established the agency's portfolio management practice. Implemented Governance process across the entire organization. Integrated IT portfolios with Strategy, budget, enterprise architecture, and project management. Hosted quarterly Investment Board meetings to prioritize IT portfolios. Participated in the organization's strategic planning. Established investment selection criteria and performance measurement metrics. Assisted IT budget planning for three fiscal years.

Work History

Grant Thornton LLP, Director, Global Public Sector, October 2009 – present
Serco Inc., Director, Portfolio Management Practice, June 2008 – October 2009

Robbins Gioia, Director, Investment Management Practice, January 2004 – March 2008

Fujitsu Consulting, Associate Director, Project Management, November 2000 – January 2004

Education and Certifications

M.B.A., University of Maryland, 1997

B.S., Computer Information Systems, Southern New Hampshire University, 1994

Project Management Professional (PMP)

IT service management (ITIL) Foundation level certificate

Six Sigma Green Belt

Kellogg Business School Portfolio Management Executive

Xavier Bignon, CMQ/OE, PMP, CSSBB, CQA, ITIL v3, CSTE, CSQA

Why Selected for this Role?

- Mr. Bignon holds two Master's degree in Industrial Systems Engineering and Innovation Management.
- Mr. Bignon holds certifications in Quality & Organizational Excellence (ASQ – CMQ/OE), Certified Six Sigma Black Belt (ASQ – CSSBB), Certified Quality Auditor (ASQ – CQA), Certified Project Management Professional (PMI – PMP), Certified Six Sigma Green Belt (ASQ – CSSGB), Certified Software Quality Analyst (QAI – CSQA), Certified Software Tester (QAI – CSTE), and Certified ITIL Professional Foundation Level.
- Mr. Bignon has over ten years combined experience in IT systems management and business process improvement for government and private IT organizations.
- He has expertise in business process modeling, quality assurance standards and quality control of systems.
- Mr. Bignon has broad knowledge of customer relationship management systems, content and knowledge management, and IT service based standards.
- He is also experienced in agile projects management, management of industry certification programs (ISO 9001, ISO 20000 and CMMI for Services), development and implementation of policies and procedures in all areas of quality control and assurance processes, and management of deployment and customer acceptance of IT solutions.

Relevant Experience

- ***Department of Commerce*** – U.S. Patent and Trade Office (June 2015 – present) Manages the United States Patent and Trade Office OCIO activity based costing model in SAP Performance Cost Management Tool. Ensures alignment between OCIO data requirements and Activity-Based Information (ABI) model structure. Leads adjustment and improvement activities using IT and ABC best practices. Provides activity based costing (ABC) support, financial analysis/IT fee studies/reporting. Produces quarterly financial closing documents and reports related to OCIO activities.

U.S. Department of the Veterans Affairs – Led a team of 3 project managers focused on Change Management, Knowledge Management and Process Improvement within the U.S. Department of the Veterans Affairs. Performed capacity assessments and functional internal audits. Implemented record management and automation by leveraging MS SharePoint. Trained VA personnel on process management practices. Responsible for the business analysis and quality assurance technical writing in five proposals leading to two awards. As Test Manager for the Veterans Relationship Management at U.S Department of the Veterans Affairs, led a team of 4 testers responsible for MS CRM Dynamics and eGain Knowledge Management acceptance testing and deployment process for the VBA National Call Centers, Education Call Center, and VHA Northern California Call Center (8 concurrent projects, over \$20 million in implementation funding). Piloted, implemented, configured and trained over 50 PMO and IT staff members on IBM Rational Jazz SDLC platform. Advised the Testing & Deployment Chief and deputy Director on product readiness, test strategy and process improvement.

- ***Definitive Logic*** – Internal auditor, managed auditing process, leading to achievement of ISO 9001:2008 certification and CMMI maturity level 3 for development. Developed internal IT standards, IT change management and performance reporting to Definitive Logic Executives. Identified and deploy appropriate infrastructure, tools and trainings supporting the practice.
- ***U.S Army Corps of Engineers Real Estate Division*** – As business process engineer, developed “As-Is” & “To-Be” Real Estate management process models in BPMN 2.0. Performed quantitative gap analysis and performance metrics baseline through process simulation. Created business process architecture leading to follow-up IT development projects using IBM Tririga.
- ***Federal Communication Commission*** – Led and completed a six sigma project on a customer relationship management development project at the Employer Support for the Guard and Reserve (ESGR), reducing by 80% production defects in six months, realizing a cost saving of 1 FTE (\$145K) for a team of four. Led on-site JAD session with product stakeholders for Test Driven Development (TDD) activities. Developed and implemented test automation against Drupal content management system at the Federal Communication Commission based on Open Source software as part of the “Open Gov” initiative.
- ***MetroStar Systems Inc.*** – Initiated and managed the ISO 20000-2008 certification process for the IT Service delivery site in Stafford Office and developed the company’s IT risk management tool as part of the PMO. Developed and conducted initial IT service assessment in preparation of the ISO audit.

Work History

- | | |
|---|---|
| ▪ Grant Thornton LLP, Senior Associate, Global Public Sector, June 2015–present | ▪ Associated Veterans LLC, Senior Project Manager, November 2011-January 2013 |
| ▪ Definitive Logic, Senior Consultant, January 2013- June 2015 | ▪ MetroStar Systems Inc., Quality Assurance Lead, August 2010 - November 2011 |

Education and Certifications

M.S., Industrial Systems Engineering, ENSGSI, France 2003

M.S., Innovation Management, INPL, France 2003

Certified Manager of Quality & Organizational Excellence (ASQ – CMQ/OE)

Certified Six Sigma Black Belt (ASQ – CSSBB)

Certified Quality Auditor (ASQ – CQA)

Certified Project Management Professional (PMI – PMP)

Certified Six Sigma Green Belt (ASQ – CSSGB)

Certified Software Quality Analyst (QAI – CSQA)

Certified Software Tester (QAI – CSTE)

Certified ITIL Professional Foundation Level

ASQ Training – Improving Customer Experience, 2015

ASQ Training – Auditing against ISO 17025 (testing laboratories), 2014

Business Process Modeling Notation 2.0 (BPMN 2.0) Training, 2013

ASQ Training – Design of Experiments, 2013

MS Project Training, 2011

SEI - CMMI 1.2 Svc, SEI – CMMI 1.3 upgrade Training, 2010

SEI - CMMI 1.2 Dev Training, 2009

Test Process Improvement (TPI)®, 2009

Don Michie, Intel Project Management Certification, Lean Six Sigma Green Belt

Why Selected for this Role?

- Mr. Michie holds a degree in Software Engineering.
- Mr. Michie is a C Level executive with over 30 years of IT and leadership experience.
- His expertise across Strategy, Applications and Operations has delivered successful solutions for Fortune 50 companies as well as public sector clients.
- His breadth of experience includes Enterprise Architecture that leverage best practices frameworks and methodologies to drive reuse cost savings, governance and alignment to business partner initiatives.
- He is experienced in IT Service Management (ITSM), Testing Methodologies and Frameworks for complex distributed systems, Service Oriented Architecture (SOA), Integration Architecture, SAP, Supply Chain Transformation, Business Process Reengineering, Program/Project Management, Application Development, and Organizational Change Leadership.
- In addition, he has over 16 years of experience adapting and adopting Enterprise Architecture Frameworks and Architecture Development methodologies including FEAF, DODAF, E2AF, TOGAF and Zachman for clients in both private and public sector, including Intel, Alberta Treasury Bank and Accenture, the Department of Health Care Services, CalPERS, California Department of Technology and Oregon Health Authority.

Relevant Experience

- ***State of Hawaii*** – Project Manager and Senior Consultant for IT Service Management as part of Gartner IT Readiness initiative; Created IT Service Management Charter for HI State Office of Information Technology (OIT) for Service Desk, Incident Management, Change Management and Request Fulfillment.
- ***Department of Healthcare Services*** – Senior Consultant, Application Performance Management; Project Manager and Lead Architect for Infrastructure and Application Performance Management initiative; Assessed existing monitoring capabilities as well as associated support agreements with vendors to establish baseline; Conducted Map/Gap analysis of existing capabilities against Gartner MQ vendor capabilities
- ***California Public Employees Retirement System Sacramento, CA*** – Consultant Test Methodology, ITSM and HP QC/ALM Architect; Project Manager for the Test Methodology and IT Service Management engagement; Assessed Release Management, Change Management, Capacity Planning and Software Development Lifecycle (SDLC); Provided strategic roadmap based on assessment recommendations; Provided “As Is” and “To Be” processes for Release Management, Change Management, Capacity Planning and SDLC; Developed ITIL V3 based Change Management process.
- ***California Department of Health Care Services*** – Consultant Release Management Office, Enterprise Architecture; Project manager for the Release Management (RMO) engagement; Created HP ALM Architecture and implemented and trained HP ALM; Wrote and trained DHCS staff and executives on ALM and Testing Center of Excellence; Develop Testing and Quality Service Center of Excellence framework, means and methods.

Interlocked to Enterprise Test Office (ETO) and Enterprise Architecture framework; Develop recommended organization changes for the ETO and the Release Management Office (RMO) and ensured ETO Test Strategy is compliant with IEEE829 standards and ISO 20000 standard for ITIL V3 interlock.

Work History

- State of Hawaii, Senior Consultant, IT Service Management, March 2015 – August 2015
- Department of Healthcare Services, Senior Consultant, Application Performance Management, January 2014 – March 2016
- California Public Employees Retirement System, Consultant Test Methodology, ITSM and HP QC/ALM Architect, January 2014 – August 2014
- California Department of Health Care Services, Consultant, Enterprise Architecture, January 2011 – January 2014

Education and Certifications

Bachelor of Science – Software Engineering – Canterbury University, Sussex UK 2001

Intel Project Management Certification (2005)

Lean Six Sigma Green Belt (2006) Certification (CERT)

**EXHIBIT A-2
WORK AUTHORIZATION FORM**

The task/deliverable(s) will be performed in accordance with this Work Authorization and the provision of Contract Number: **16-10645**

WORK AUTHORIZATION NUMBER	PAGE(S) of
---------------------------	-------------------

TITLE OF TASK/DELIVERABLE

TASK/DELIVERABLE SUMMARY *(Brief description of task/deliverable to be performed under work authorization)*

START DATE	COMPLETION DATE
TOTAL ESTIMATED LABOR HOURS	TOTAL ESTIMATED COST

APPROVALS

CONTRACTOR CONTRACT ADMINISTRATOR NAME	TITLE
--	-------

SIGNATURE	DATE
-----------	------

DEPARTMENT OF TECHNOLOGY CONTRACT ADMINISTRATOR NAME	TITLE
--	-------

SIGNATURE	DATE
-----------	------

The following pages are not mandatory, as long as the task/deliverable summary on the WA form is detailed, but highly recommended.

1. TASK/DELIVERABLE SUMMARY INFORMATION

SUMMARY			
Task/Deliverable Number			
Task/Deliverable Name			
Version Number			
Total Review Time for Draft and Final Document Task/Deliverable in State Business Days	Total Review Time	Draft Review	Final Review
Delivery/Format			
Number of Copies			
Intended Audience			

2. INTRODUCTION

3. REQUIREMENTS

3.1. REQUIREMENTS DESCRIPTION

3.2. SPECIAL REQUIREMENTS/CLARIFICATIONS

4. TASK/DELIVERABLE CONTENT

4.1. SCOPE

4.2. DESCRIPTION

Project Management Approval – Section where approval signatures are gathered. There should be two tables for review log and management approval signatures.

Table 1.1 Task/Deliverable Review History Log

TAKS/DELIVERABLE REVIEW HISTORY LOG		
Reviewer/Role	Date	Comments

Table 1.2 Task/Deliverable Project Management Approval

TASK/DELIVERABLE XXXX		
Approver/Role	Date	Signature
Project Manager		
Comments:		

4.3. REFERENCED DOCUMENTS

4.4. CRITICAL DEPENDENCIES

4.5. RESOURCES

- The following table lists the key resources by organization required to achieve a successful signoff on Task/Deliverable XXXX.

STATE KEY RESOURCES	
Role	Responsibilities
OTech Project Manager	Responsible for Acceptance of the Final Task/Deliverable.
OTech Project Director	Responsible for Senior Leadership review and approval.
XXXX Project Manager	Responsible for Senior Leadership review and approval.

VENDOR KEY RESOURCES	
Role	Responsibilities
Vendor Project Manager	Responsible for Quality Assurance review.

**EXHIBIT A-4
WORK AUTHORIZATION ACCEPTANCE DOCUMENT**

CONTRACTOR NAME: Grant Thornton, LLP

DEPARTMENT OF TECHNOLOGY CONTRACT NUMBER: 16-10645

WORK AUTHORIZATION ACCEPTANCE DOCUMENT (WAAD) NUMBER: _____

WORK AUTHORIZATION TITLE: _____

WORK AUTHORIZATION COMPLETION DATE: _____

TOTAL COST OF WORK AUTHORIZATION: \$ _____

WORK AUTHORIZATION DESCRIPTION:

DEPARTMENT OF TECHNOLOGY ACCEPTANCE OR REJECTION:

AUTHORIZED AND APPROVED:

CONTRACTOR OFFICIAL SIGNATURE / DATE

DEPARTMENT OF TECHNOLOGY
CONTRACT ADMINISTRATOR SIGNATURE /
DATE

Note: Once the Contractor and the Department of Technology have approved the WAAD as stipulated in the contract, the Contractor may submit an invoice to the Department of Technology. Refer to payment terms in Exhibit B.

EXHIBIT B
BUDGET DETAIL AND PAYMENT PROVISIONS

1. Payment for services performed under this Contract shall be Hourly by Work Authorization. It shall be the CDT's sole determination as to whether a task/deliverable has been successfully completed and is acceptable. A signed WA Acceptance Document, Exhibit A-4 is required from the CDT Contract Administrator before processing an invoice for payment.
2. Upon successful completion and acceptance of each project task/deliverable identified in a WA, the Contractor will submit an invoice for payment associated with the individual payment amounts. Payment shall be based on the cost worksheet and acceptance by the CDT.
3. Invoices shall be submitted in triplicate, and shall identify labor and costs charged for each approved WA. Invoices shall be submitted monthly, in arrears, identifying Contractor personnel by name and classification, hourly rate of pay and hours expended; however, invoices shall be due and payable, and payment shall be made, only after the CDT acceptance of hours worked or completion of each WA under this Contract.
4. The Contractor costs related to items such as travel and per diem are costs of the Contractor, shall be inclusive of the hourly rate bid, and **will not be paid separately** as part of this Contract.
5. Submit your invoice using ONE of the following options referencing the Contract Number or Agency Order Number:
 - a. Send via U.S. Mail in **TRIPLICATE** to:
California Department of Technology
Financial Management Branch – Accounting Office
P.O. Box 1810
Rancho Cordova, CA 95741
 - OR**
 - b. Send electronically to: APInvoices@state.ca.gov
6. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Contract does not appropriate sufficient funds for the program, this Contract shall be of no further force and effect. In this event, the State shall have no liability to pay any funds whatsoever to the Contractor or to furnish any other considerations under this Contract and Contractor shall not be obligated to perform any provisions of this Contract.
7. If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, the State shall have the option to either cancel this Contract with no liability occurring to the State, or offer a contract amendment to the Contractor to reflect the reduced amount.
8. Payment will be made in accordance with, and within the time specified in, Government Code Chapter 4.5, commencing with Section 927. Payment to small/micro businesses shall be made in accordance with and within the time specified in Chapter 4.5, Government Code 927 et seq.

EXHIBIT B-1
COST WORKSHEET

The Contractor shall provide all labor, materials, and equipment necessary to provide the consulting services for **the CDT/OTech Shared Services and Financial Review** in accordance with the specifications described in the SOW, Exhibit A, at the rates specified below. **Payment for services performed under this contract shall be hourly by WA.** Submission of this information is required.

Staff Name	IT MSA Classification	*Rate Per Hour
Wei Tang	Senior Project Manager	\$180.00
Xavier Bignon	Senior Project Manager	\$180.00
Donald Michie	Senior Technical Lead	\$160.00

EXHIBIT D

SPECIAL TERMS AND CONDITIONS TO SAFEGUARD FEDERAL TAX INFORMATION

Federal statute, regulations and guidelines require that all contracts for services relating to the processing, storage, transmission, or reproduction of federal tax returns or return information, the programming, maintenance, repair, or testing of equipment or other property, or the providing of other services, for tax administration purposes include the provisions contained in this exhibit. (See 26 U.S.C. §6103(n); 26 C.F.R. §301.6103(n)-1(a)(2) and (d); Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies (Rev. 8-2010), Section 5.5 and Exhibit 7.)

The contractor agrees to comply with 26 U.S.C. §6103(n); 26 C.F.R. §301.6103(n)-1; IRS Publication 1075 (Rev. 8-2010); and all applicable conditions and restrictions as may be prescribed by the IRS by regulation, published rules or procedures, or written communication to the contractor. (See 26 C.F.R. §301.6103(n)-1(d); IRS Publication 1075 (Rev. 8-2010).)

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be done under the supervision of the contractor or the contractor's employees.
- (2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
- (3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (4) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- (6) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.

(7) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.

(8) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(9) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any

manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information* and Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.¹

III. INSPECTION

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

REFERENCES

26 U.S.C. §6103(n)

Pursuant to regulations prescribed by the Secretary, returns and return information may be disclosed to any person, including any person described in section 7513 (a), to the extent necessary in connection with the processing, storage, transmission, and reproduction of such returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and the providing of other services, for purposes of tax administration.

26 C.F.R. §301.6103(n)-1 Disclosure of returns and return information in connection with procurement of property and services for tax administration purposes.

(a) *General rule.* Pursuant to the provisions of section 6103(n) of the Internal Revenue Code and subject to the requirements of paragraphs (b), (c), and (d) of this section, officers or employees of the Treasury Department, a State tax agency, the Social Security Administration, or the Department of Justice, are authorized to disclose returns and return information (as defined in section 6103(b)) to any person (including, in the case of the Treasury Department, any person described in section 7513(a)), or to an officer or employee of such person, to the extent necessary in connection with contractual procurement of:

- (1) Equipment or other property, or
- (2) Services relating to the processing, storage, transmission, or reproduction of such returns or return information, the programming, maintenance, repair, or testing of equipment or

other property, or the providing of other services, for purposes of tax administration (as defined in section 6103(b)(4)).

No person, or officer or employee of such person, to whom a return or return information is disclosed by an officer or employee of the Treasury Department, the State tax agency, the Social Security Administration, or the Department of Justice, under the authority of this paragraph shall in turn disclose such return or return information for any purpose other than as described in this paragraph, and no such further disclosure for any such described purpose shall be made by such person, officer, or employee to anyone, other than another officer or employee of such person whose duties or responsibilities require such disclosure for a purpose described in this paragraph, without written approval by the Internal Revenue Service.

(b) *Limitations.* For purposes of paragraph (a) of this section, disclosure of returns or return information in connection with contractual procurement of property or services described in such paragraph will be treated as necessary only if such procurement or the performance of such services cannot otherwise be reasonably, properly, or economically carried out or performed without such disclosure.

Thus, for example, disclosures of returns or return information to employees of a contractor for purposes of programming, maintaining, repairing, or testing computer equipment used by the Internal Revenue Service or a State tax agency should be made only if such services cannot be reasonably, properly, or economically performed by use of information or other data in a form which does not identify a particular taxpayer. If, however, disclosure of returns or return information is in fact necessary in order for such employees to reasonably, properly, or economically perform the computer related services, such disclosures should be restricted to returns or return information selected or appearing at random. Further, for purposes of paragraph (a), disclosure of returns or return information in connection with the contractual procurement of property or services described in such paragraph should be made only to the extent necessary to reasonably, properly, or economically conduct such procurement activity. Thus, for example, if an activity described in paragraph (a) can be reasonably, properly, and economically conducted by disclosure of only parts or portions of a return or if deletion of taxpayer identity information (as defined in section 6103(b)(6) of the Code) reflected on a return would not seriously impair the ability of the contractor or his officers or employees to conduct the activity, then only such parts or portions of the return, or only the return with taxpayer identity information deleted, should be disclosed.

(c) *Notification requirements.* Persons to whom returns or return information is or may be disclosed as authorized by paragraph (a) of this section shall provide written notice to their officers or employees—

- (1) That returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized by paragraph (a) of this section;
- (2) That further inspection of any returns or return information for a purpose or to an extent unauthorized by paragraph (a) of this section constitutes a misdemeanor, punishable upon conviction by a fine of as much as \$1,000, or imprisonment for as long as 1 year, or both, together with costs of prosecution;

¹ A 30 minute disclosure awareness training video produced by the IRS can be found at

<http://www.irsvideos.gov/Governments/Safeguards/DisclosureAwarenessTrainingPub4711>

(3) That further disclosure of any returns or return information for a purpose or to an extent unauthorized by paragraph (a) of this section constitutes a felony, punishable upon conviction by a fine of as much as \$5,000, or imprisonment for as long as 5 years, or both, together with the costs of prosecution;

(4) That any such unauthorized further inspection or disclosure of returns or return information may also result in an award of civil damages against any person who is not an officer or employee of the United States in an amount not less than \$1,000 for each act of unauthorized inspection or disclosure or the sum of actual damages sustained by the plaintiff as a result of such unauthorized disclosure or inspection as well as an award of costs and reasonable attorneys fees; and

(5) If such person is an officer or employee of the United States, a conviction for an offense referenced in paragraph (c)(2) or (c)(3) of this section shall result in dismissal from office or discharge from employment.

(d) *Safeguards.* Any person to whom a return or return information is disclosed as authorized by paragraph (a) of this section shall comply with all applicable conditions and requirements which may be prescribed by the Internal Revenue Service for the purposes of protecting the confidentiality of returns and return information and preventing disclosures of returns or return information in a manner unauthorized by paragraph (a). The terms of any contract between the Treasury Department, a State tax agency, the Social Security Administration, or the Department of Justice, and a person pursuant to which a return or return information is or may be disclosed for a purpose described in paragraph (a) shall provide, or shall be amended to provide, that such person, and officers and employees of the person, shall comply with all such applicable conditions and restrictions as may be prescribed by the Service by regulation, published rules or procedures, or written communication to such person. If the Service determines that any person, or an officer or employee of any such person, to whom returns or return information has been disclosed as provided in paragraph (a) has failed to, or does not, satisfy such prescribed conditions or requirements, the Service may take such actions as are deemed necessary to ensure that such conditions or requirements are or will be satisfied, including—

(1) Suspension or termination of any duty or obligation arising under a contract with the Treasury Department referred to in this paragraph or suspension of disclosures by the Treasury Department otherwise authorized by paragraph (a) of this section, or

(2) Suspension of further disclosures of returns or return information by the Service to the State tax agency, or to the Department of Justice, until the Service determines that such conditions and requirements have been or will be satisfied.

(e) *Definitions.* For purposes of this section—

(1) The term *Treasury Department* includes the Internal Revenue Service and the Office of the Chief Counsel for the Internal Revenue Service;

(2) The term *State tax agency* means an agency, body, or commission described in section 6103(d) of the Code; and

(3) The term *Department of Justice* includes offices of the United States Attorneys.

IRS Publication 1075 (Rev. 8-2010) Section 5.5 Control over Processing

Processing of FTI, in an electronic media format, including removable media, microfilms, photo impressions, or other formats (including tape reformatting or reproduction or conversion to punch cards, digital images or hard copy printout) will be performed pursuant to one of the following procedures:

5.5.1 Agency Owned and Operated Facility

Processing under this method will take place in a manner that will protect the confidentiality of the information on the electronic media. All safeguards outlined in this publication also must be followed and will be subject to IRS safeguard reviews.

5.5.2 Contractor or Agency Shared Facility – Consolidated Data Centers

Recipients of FTI are allowed to use a shared facility but only in a manner that does not allow access to FTI by employees, agents, representatives or contractors of other agencies using the shared facility.

Note: For purposes of applying sections 6103(l), (m) and (n), the term “agent” includes contractors. Access restrictions pursuant to the IRC authority by which the FTI is received continue to apply. For example, since human services agencies administering benefit eligibility programs may not allow contractor access to any FTI received, their data within the consolidated data center may not be accessed by any contractor of the data center.

The requirements in Exhibit 7, Contract Language for General Services, must be included in the contract in accordance with IRC Section 6103(n).

The contractor or agency-shared computer facility is also subject to IRS safeguard reviews.

Note: The above rules also apply to releasing electronic media to a private contractor or other agency office even if the purpose is merely to erase the old media for reuse.

Agencies utilizing consolidated data centers must implement appropriate controls to ensure the protection of FTI, including a service level agreement (SLA) between the agency authorized to receive FTI and the consolidated data center. The SLA should cover the following:

The consolidated data center is considered to be a “contractor” of the agency receiving FTI. The agency receiving FTI – whether it is a state revenue, workforce, child support enforcement or human services agency – is responsible for ensuring the protection of all FTI received. However, as the “contractor” for the agency receiving FTI, the consolidated data center shares responsibility for safeguarding FTI as well.

Provide written notification to the consolidated data center management that they are bound by the provisions of Publication 1075, relative to protecting all federal tax information within their possession or control. The SLA should also include details concerning the consolidated data center’s responsibilities during a safeguard review and support required to resolve identified findings.

The agency will conduct an internal inspection of the consolidated data center every eighteen months (see section 6.3). Multiple agencies sharing a consolidated data center may partner together to conduct a single, comprehensive internal inspection. However, care

should be taken to ensure agency representatives do not gain unauthorized access to other agency's FTI during the internal inspection.

The employees from the consolidated data center with access to FTI, including system administrators and programmers, must receive disclosure awareness training prior to access to FTI and annually thereafter and sign a confidentiality statement. This provision also extends to any contractors hired by the consolidated data center that has access to FTI.

The specific data breach incident reporting procedures for all consolidated data center employees and contractors. The required disclosure awareness training must include a review of these procedures.

The Exhibit 7 language must be included in the contract between the recipient agency and the consolidated data center, including all contracts involving contractors hired by the consolidated data center.

Identify responsibilities for coordination of the 45-day notification of the use of contractors or sub-contractors with access to FTI.

Note: Generally, consolidated data centers are either operated by a separate state agency (example: Department of Information Services) or by a private contractor. If an agency is considering transitioning to either a state owned or private vendor consolidated data center, the Office of Safeguards strongly suggests the agency submit a request for discussions with Safeguards as early as possible in the decision-making or implementation planning process. The purpose of these discussions is to ensure the agency remains in compliance with safeguarding requirements during the transition to the consolidated data center.

26 U.S.C. §7213. Unauthorized disclosure of information

(a) Returns and return information

(1) Federal employees and other persons

It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)). Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) State and other employees

It shall be unlawful for any person (not described in paragraph (1)) willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)) acquired by him or another person under subsection (d), (i)(3)(B)(i) or (7)(A)(ii), (l)(6), (7), (8), (9), (10), (12), (15), (16), (19), or (20) or (m)(2), (4), (5), (6), or (7) of section 6103.

Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(3) Other persons

It shall be unlawful for any person to whom any return or return information (as defined in section 6103(b)) is disclosed in a manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a

felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(4) Solicitation

It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information (as defined in section 6103(b)) and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(5) Shareholders

It shall be unlawful for any person to whom a return or return information (as defined in section 6103(b)) is disclosed pursuant to the provisions of section 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not to exceed \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(b) Disclosure of operations of manufacturer or producer

Any officer or employee of the United States who divulges or makes known in any manner whatever not provided by law to any person the operations, style of work, or apparatus of any manufacturer or producer visited by him in the discharge of his official duties shall be guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than \$1,000, or imprisoned not more than 1 year, or both, together with the costs of prosecution; and the offender shall be dismissed from office or discharged from employment.

(c) Disclosures by certain delegates of Secretary

All provisions of law relating to the disclosure of information, and all provisions of law relating to penalties for unauthorized disclosure of information, which are applicable in respect of any function under this title when performed by an officer or employee of the Treasury Department are likewise applicable in respect of such function when performed by any person who is a "delegate" within the meaning of section 7701(a)(12)(B).

(d) Disclosure of software

Any person who willfully divulges or makes known software (as defined in section 7612(d)(1)) to any person in violation of section 7612 shall be guilty of a felony and, upon conviction thereof, shall be fined not more than \$5,000, or imprisoned not more than 5 years, or both, together with the costs of prosecution.

(e) Cross references

(1) Penalties for disclosure of information by preparers of returns
For penalty for disclosure or use of information by preparers of returns, see section 7216.

(2) Penalties for disclosure of confidential information

For penalties for disclosure of confidential information by any officer or employee of the United States or any department or agency thereof, see 18 U.S.C. 1905.

26 U.S.C. §7213A. Unauthorized inspection of returns or return information

(a) Prohibitions

(1) Federal employees and other persons

It shall be unlawful for—

(A) any officer or employee of the United States, or

(B) any person described in subsection (l)(18) or (n) of section 6103 or an officer or employee of any such person, willfully to inspect, except as authorized in this title, any return or return information.

(2) State and other employees

It shall be unlawful for any person (not described in paragraph (1)) willfully to inspect, except as authorized in this title, any return or return information acquired by such person or another person under a provision of section 6103 referred to in section 7213 (a)(2) or under section 6104 (c).

(b) Penalty

(1) In general

Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding \$1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) Federal officers or employees

An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) Definitions

For purposes of this section, the terms "inspect", "return", and "return information" have the respective meanings given such terms by section 6103 (b).

26 U.S.C. §7431. Civil damages for unauthorized inspection or disclosure of returns and return information

(a) In general

(1) Inspection or disclosure by employee of United States

If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) Inspection or disclosure by a person who is not an employee of United States

If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) Exceptions

No liability shall arise under this section with respect to any inspection or disclosure -

(1) which results from a good faith, but erroneous, interpretation of section 6103, or

(2) which is requested by the taxpayer.

(c) Damages

In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of -

(1) the greater of -

(A) \$1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of -

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus

(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the costs of the action, plus

(3) in the case of a plaintiff which is described in section 7430(c)(4)(A)(ii), reasonable attorneys fees, except that if the defendant is the United States, reasonable attorneys fees may be awarded only if the plaintiff is the prevailing party (as determined under section 7430(c)(4)).

(d) Period for bringing action

Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) Notification of unlawful inspection and disclosure

If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of -

(1) paragraph (1) or (2) of section 7213(a),

(2) section 7213A(a), or

(3) subparagraph (B) of section 1030(a)(2) of title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

(f) Definitions

For purposes of this section, the terms "inspect", "inspection", "return", and "return information" have the respective meanings given such terms by section 6103(b).

(g) Extension to information obtained under section 3406

For purposes of this section -

(1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and

(2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in section 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103. For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 3406.

(h) Special rule for information obtained under section 6103(k)(9)

For purposes of this section, any reference to section 6103 shall be treated as including a reference to section 6311(e).

EXHIBIT E

SECURITY AND DATA PROTECTION

Contractor shall certify to the State compliance with applicable industry standards and guidelines, including but not limited to relevant security provisions of the California State Administrative Manual (SAM), California Statewide Information Management Manual (SIMM), The National Institute of Standards and Technology (NIST) 800-53 v4 and Federal Information Processing Standard (FIPS) Publication 199 which protect and minimize risk to the State. At a minimum, provision shall cover the following:

1. The Contractor assumes responsibility of the confidentiality, integrity and availability of the data under its control. The Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards at all times during the term of the Agreement to secure such data from data breach or loss, protect the data and information assets from breaches, introduction of viruses, disabling of devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its data or affects the integrity of that data.
2. Confidential, sensitive or personal information shall be encrypted in accordance with SAM 5350.1 and SIMM 5305-A.
3. The Contractor shall comply with statewide policies and laws regarding the use and protection of information assets and data. Unauthorized use of data by Contractor or third parties is prohibited.
4. Signed Security and Confidentiality Statement for all personnel assigned during the term of the Agreement.
5. Apply security patches and upgrades, and keep virus protection software up-to-date on all information asset on which data may be stored, processed, or transmitted.
6. The Contractor shall notify the State data owner immediately if a security incident involving the information asset occurs.
7. The State data owner shall have the right to participate in the investigation of a security incident involving its data or conduct its own independent investigation. The Contractor shall allow the State reasonable access to security logs, latency statistics, and other related security data that affects this Agreement and the State's data, at no cost to the State.
8. The Contractor shall be responsible for all costs incurred by the State due to security incident resulting from the Contractor's failure to perform or negligent acts of its personnel, and resulting in an unauthorized disclosure, release, access, review, destruction; loss, theft or misuse of an information asset. If the contractor experiences a loss or breach of data, the contractor shall immediately report the loss or breach to the State. If the State data owner determines that notice to the individuals whose data has been lost or breached is appropriate, the contractor will bear any and all costs associated with the notice or any mitigation selected by the data owner. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data.
9. The Contractor shall immediately notify and work cooperatively with the State data owner to respond timely and correctly to public records act requests.
10. The Contractor will dispose of records of State data as instructed by the State during the term of this agreement. No data shall be copied, modified, destroyed or deleted by the Contractor other than for normal operation or maintenance during the Agreement period without prior written notice to and written approval by the State.
11. Remote access to data from outside the territorial United States, including remote access to data by authorized support staff in identified support centers, is prohibited unless approved in advance by the State.
12. The physical location of Contractor's data center where the Data is stored shall be within the territorial United States.