PUBLIC
CONSULTING GROUP

Solutions that Matter

RESPONSE PACKET

State of Arkansas
Department of Human Services

Security and Privacy Control Assessment

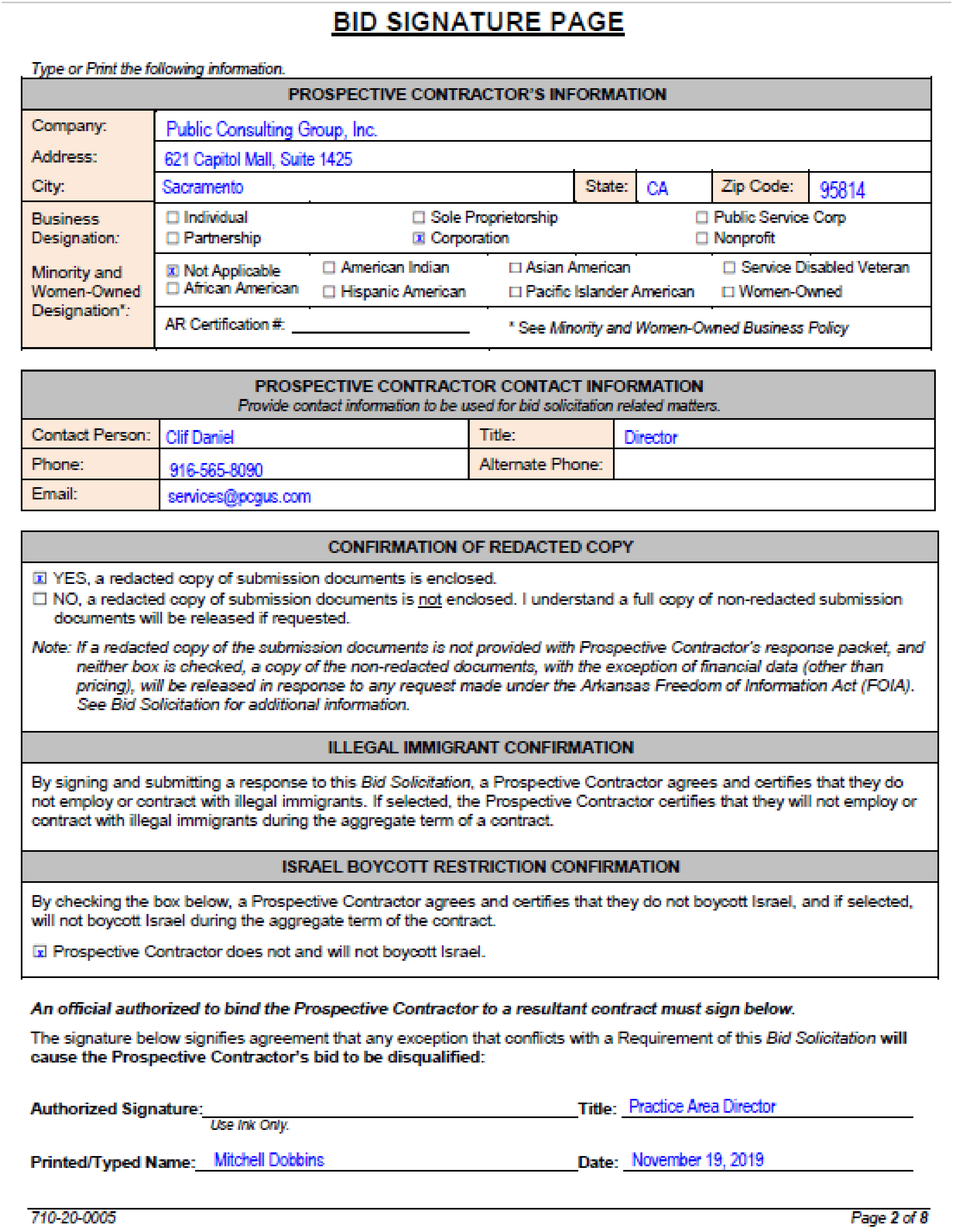
Bid No. 710-20-0005

November 22, 2019 | 2:00 PM Central

Public Consulting Group, Inc.
621 Capitol Mall, Suite 1425
Sacramento, CA 95814

Arkansas Department of Human Services
Attn: Office of Procurement
700 Main Street Slot W345
Little Rock, AR 72201

Bid Signature Page



BID SIGNATURE PAGE

Type or Print the following information.

PROSPECTIVE CONTRACTOR'S INFORMATION							
Company:	Public Consulting Group, Inc.						
Address:	621 Capitol Mall, Suite 1425						
City:	Sacramento			State:	CA	Zip Code:	95814
Business Designation:	□ Individual □ Partnership		□ Sole Proprietorship ☒ Corporation			□ Public Service Corp □ Nonprofit	
Minority and Women-Owned Designation*:	☒ Not Applicable □ African American	□ American Indian □ Hispanic American		□ Asian American □ Pacific Islander American		□ Service Disabled Veteran □ Women-Owned	
	AR Certification #: ____________		* *See Minority and Women-Owned Business Policy*				

PROSPECTIVE CONTRACTOR CONTACT INFORMATION *Provide contact information to be used for bid solicitation related matters.*			
Contact Person:	Clif Daniel	Title:	Director
Phone:	916-565-8090	Alternate Phone:	
Email:	services@pcgus.com		

CONFIRMATION OF REDACTED COPY

☒ YES, a redacted copy of submission documents is enclosed.

□ NO, a redacted copy of submission documents is not enclosed. I understand a full copy of non-redacted submission documents will be released if requested.

Note: If a redacted copy of the submission documents is not provided with Prospective Contractor's response packet, and neither box is checked, a copy of the non-redacted documents, with the exception of financial data (other than pricing), will be released in response to any request made under the Arkansas Freedom of Information Act (FOIA). See Bid Solicitation for additional information.

ILLEGAL IMMIGRANT CONFIRMATION

By signing and submitting a response to this *Bid Solicitation*, a Prospective Contractor agrees and certifies that they do not employ or contract with illegal immigrants. If selected, the Prospective Contractor certifies that they will not employ or contract with illegal immigrants during the aggregate term of a contract.

ISRAEL BOYCOTT RESTRICTION CONFIRMATION

By checking the box below, a Prospective Contractor agrees and certifies that they do not boycott Israel, and if selected, will not boycott Israel during the aggregate term of the contract.

☒ Prospective Contractor does not and will not boycott Israel.

An official authorized to bind the Prospective Contractor to a resultant contract must sign below.

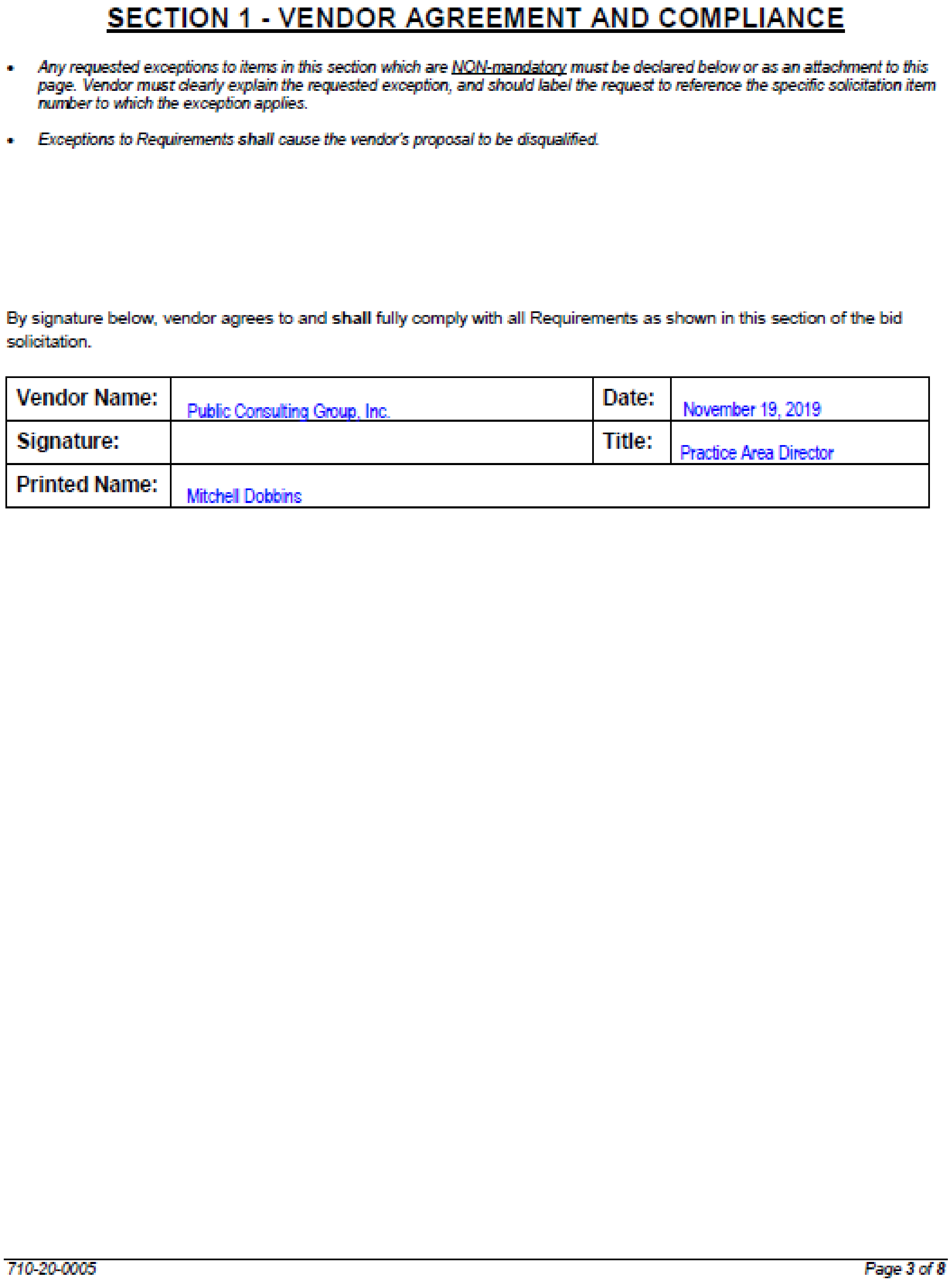
The signature below signifies agreement that any exception that conflicts with a Requirement of this *Bid Solicitation* **will cause the Prospective Contractor's bid to be disqualified:**

Authorized Signature:______________________ **Title:** Practice Area Director
Use Ink Only.

Printed/Typed Name: Mitchell Dobbins **Date:** November 19, 2019

710-20-0005 *Page 2 of 8*

SECTION 1 – VENDOR AGREEMENT AND COMPLIANCE



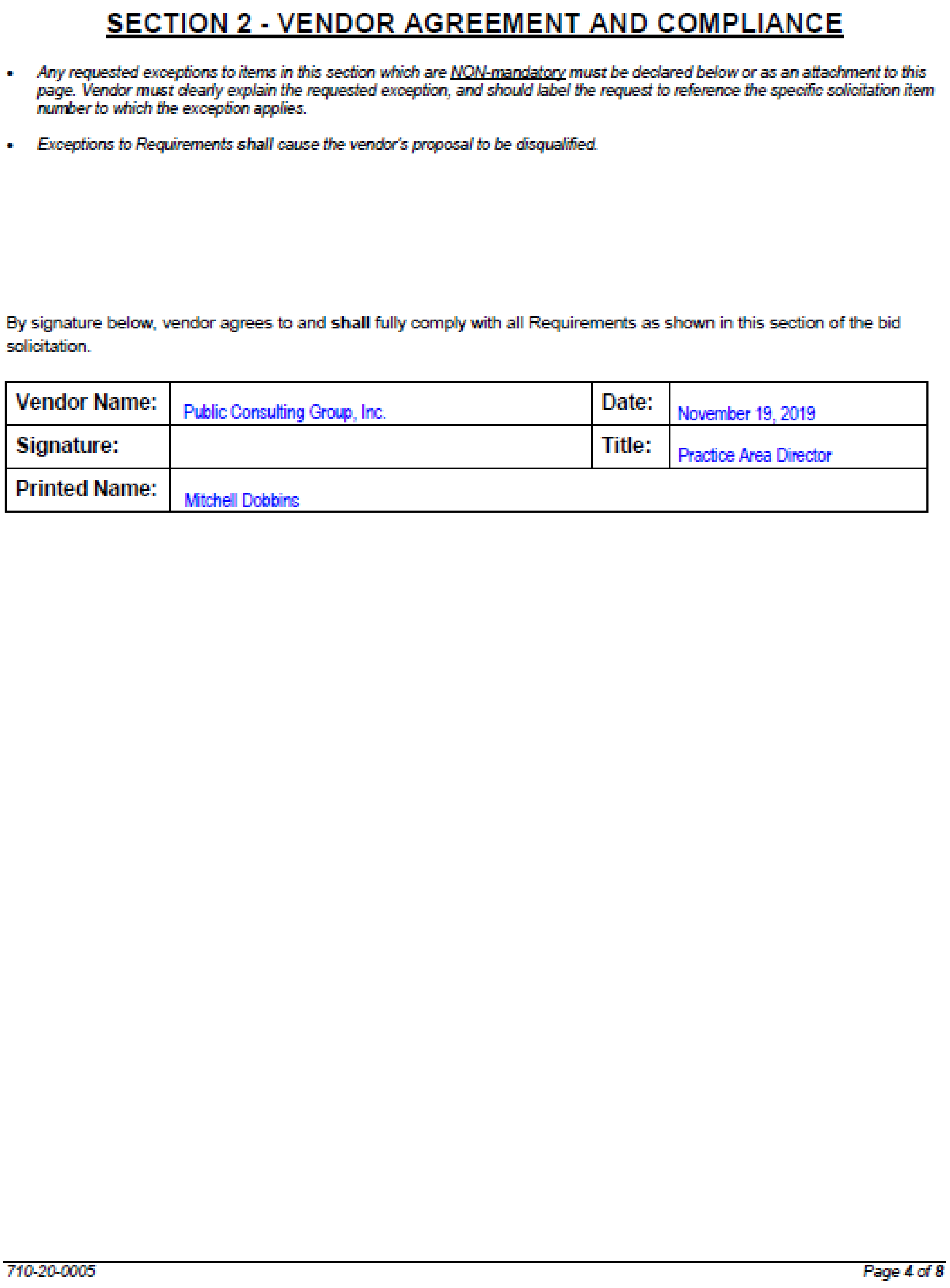
SECTION 1 - VENDOR AGREEMENT AND COMPLIANCE

- *Any requested exceptions to items in this section which are NON-mandatory must be declared below or as an attachment to this page. Vendor must clearly explain the requested exception, and should label the request to reference the specific solicitation item number to which the exception applies.*
- *Exceptions to Requirements **shall** cause the vendor's proposal to be disqualified.*

By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

Vendor Name:	Public Consulting Group, Inc.	**Date:**	November 19, 2019
Signature:		**Title:**	Practice Area Director
Printed Name:	Mitchell Dobbins		

SECTION 2 – VENDOR AGREEMENT AND COMPLIANCE



SECTION 2 - VENDOR AGREEMENT AND COMPLIANCE

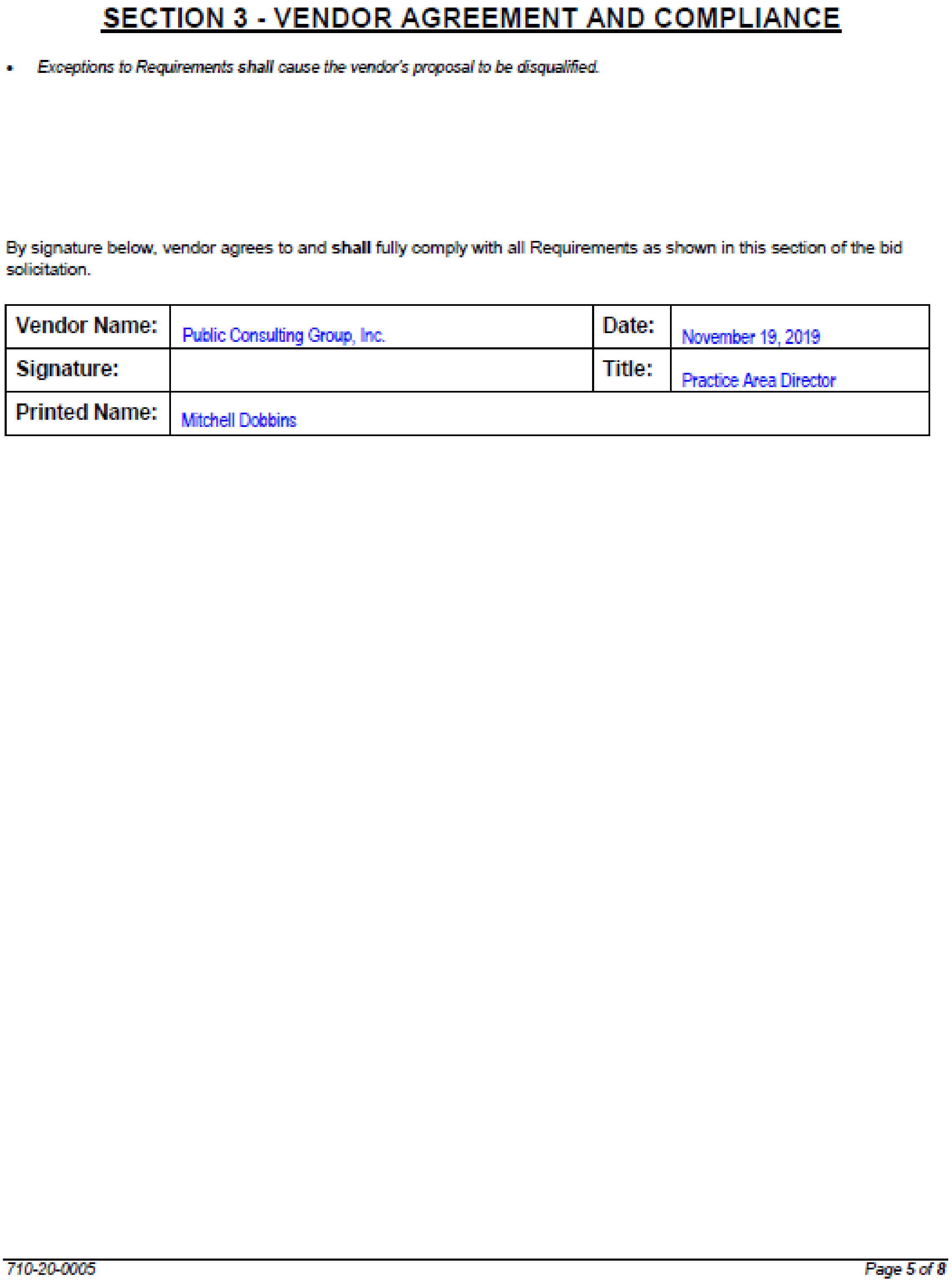
- *Any requested exceptions to items in this section which are NON-mandatory must be declared below or as an attachment to this page. Vendor must clearly explain the requested exception, and should label the request to reference the specific solicitation item number to which the exception applies.*
- *Exceptions to Requirements shall cause the vendor's proposal to be disqualified.*

By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

Vendor Name:	Public Consulting Group, Inc.	**Date:**	November 19, 2019
Signature:		**Title:**	Practice Area Director
Printed Name:	Mitchell Dobbins		

710-20-0005 *Page 4 of 8*

Section 3 – Vendor Agreement and Compliance



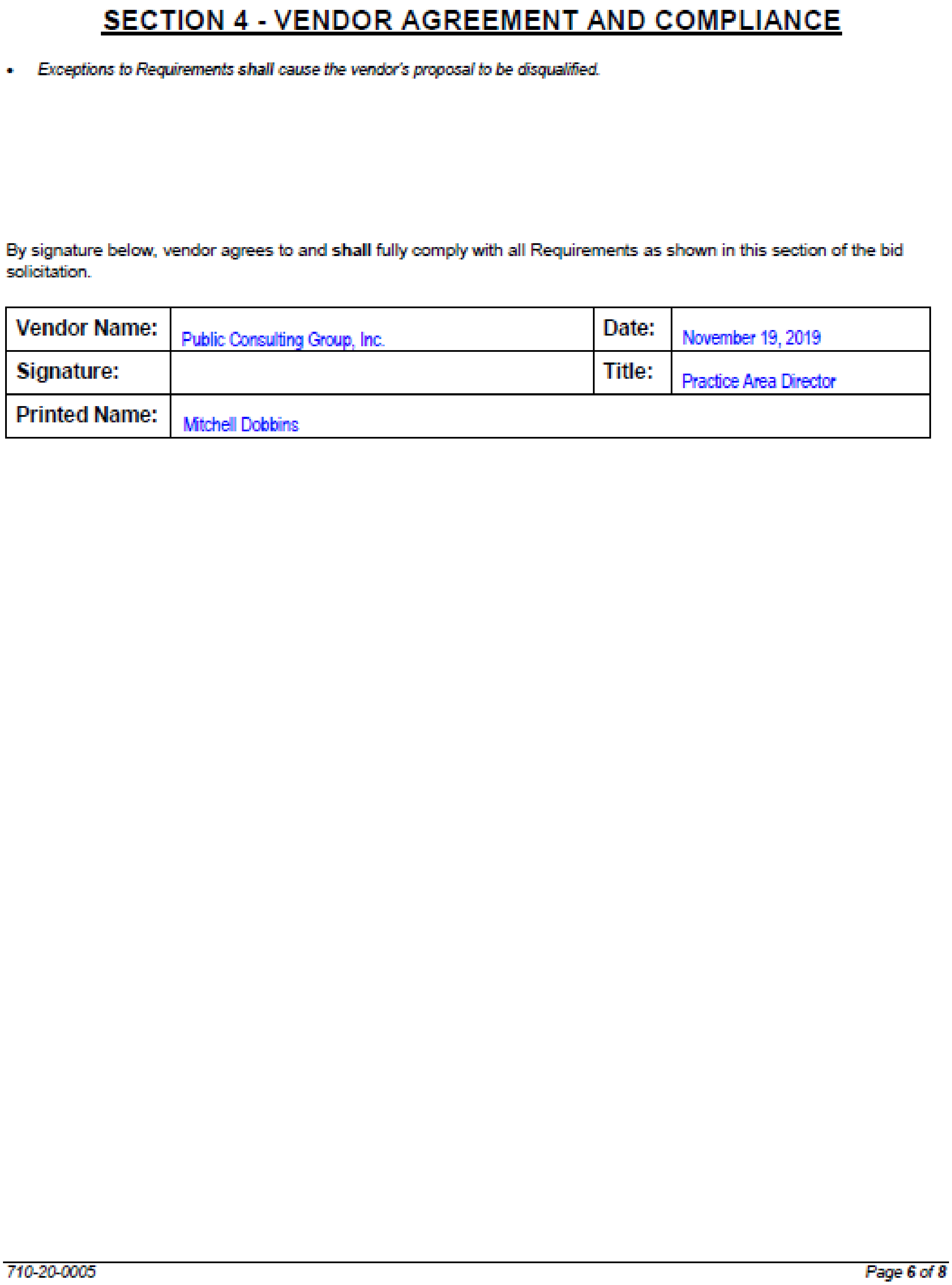
SECTION 3 - VENDOR AGREEMENT AND COMPLIANCE

- *Exceptions to Requirements **shall** cause the vendor's proposal to be disqualified.*

By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

Vendor Name:	Public Consulting Group, Inc.	**Date:**	November 19, 2019
Signature:		**Title:**	Practice Area Director
Printed Name:	Mitchell Dobbins		

Section 4 – Vendor Agreement and Compliance



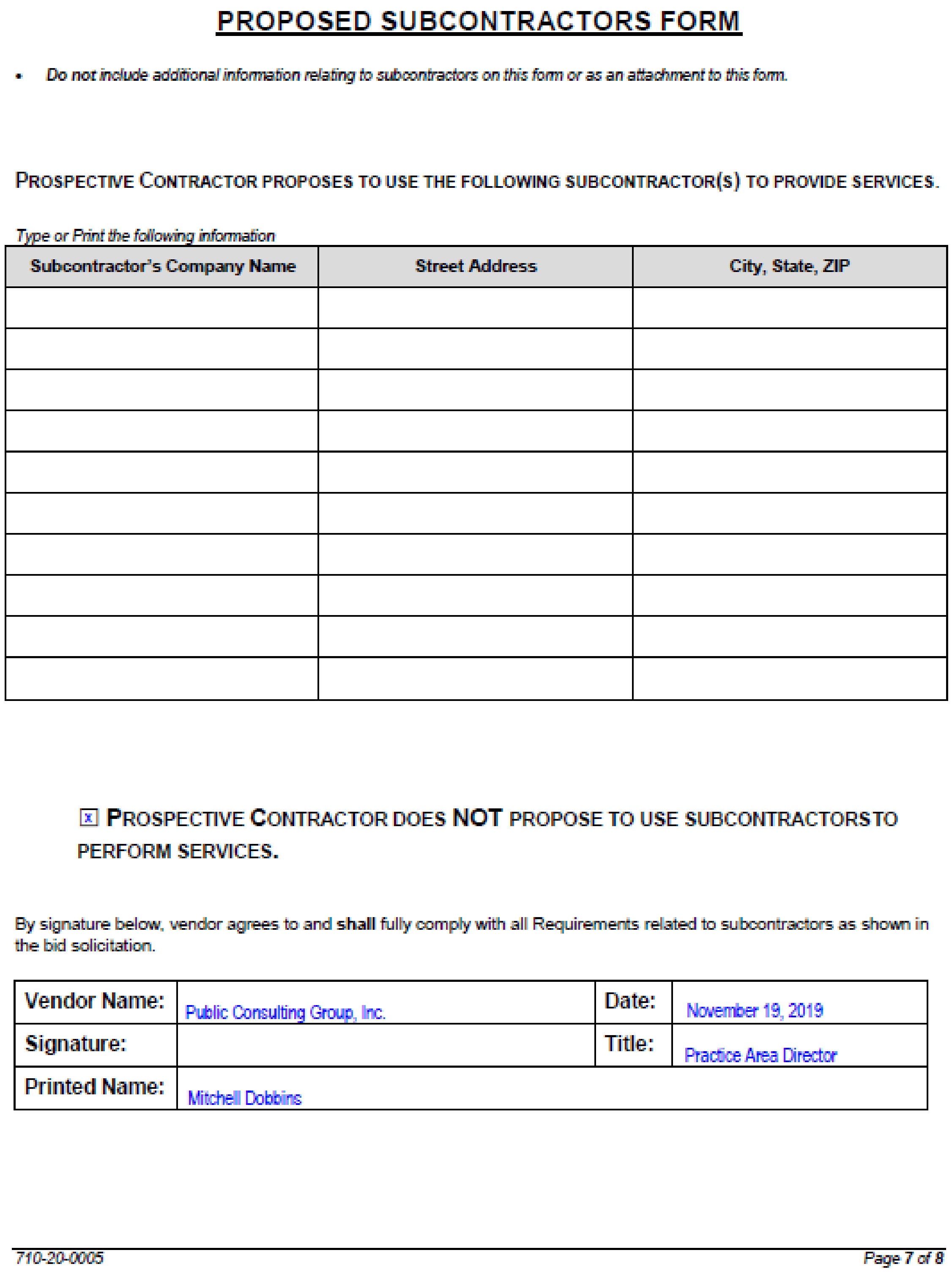
SECTION 4 - VENDOR AGREEMENT AND COMPLIANCE

- *Exceptions to Requirements **shall** cause the vendor's proposal to be disqualified.*

By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

Vendor Name:	Public Consulting Group, Inc.	**Date:**	November 19, 2019
Signature:		**Title:**	Practice Area Director
Printed Name:	Mitchell Dobbins		

Proposed Contractors Form



PROPOSED SUBCONTRACTORS FORM

- *Do not include additional information relating to subcontractors on this form or as an attachment to this form.*

PROSPECTIVE CONTRACTOR PROPOSES TO USE THE FOLLOWING SUBCONTRACTOR(S) TO PROVIDE SERVICES.

Type or Print the following information

Subcontractor's Company Name	Street Address	City, State, ZIP

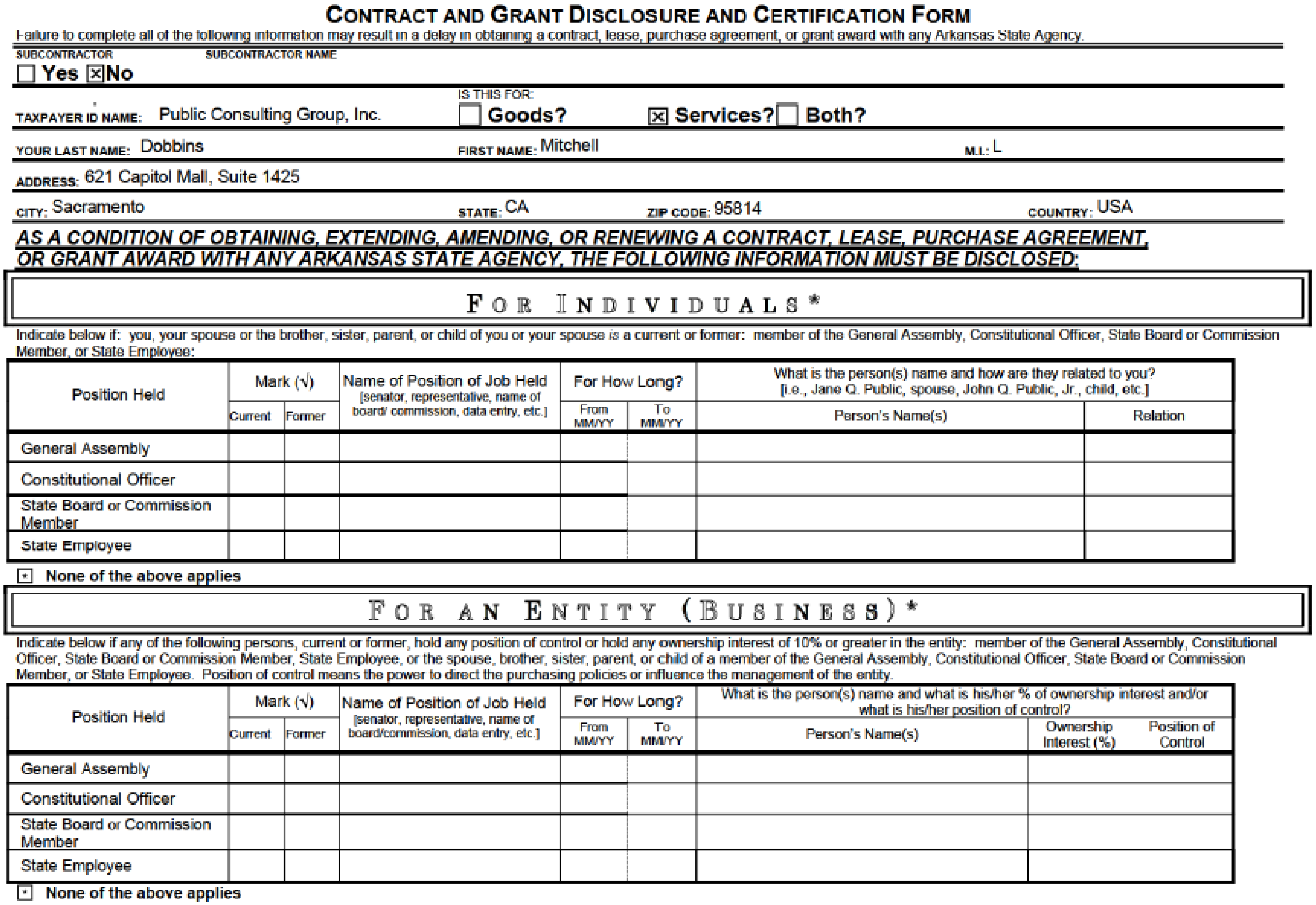
☒ PROSPECTIVE CONTRACTOR DOES **NOT** PROPOSE TO USE SUBCONTRACTORS TO PERFORM SERVICES.

By signature below, vendor agrees to and **shall** fully comply with all Requirements related to subcontractors as shown in the bid solicitation.

Vendor Name:	Public Consulting Group, Inc.	**Date:**	November 19, 2019
Signature:		**Title:**	Practice Area Director
Printed Name:	Mitchell Dobbins		

710-20-0005 *Page 7 of 8*

EO 98-04 Disclosure Form (Attachment A)



Contract and Grant Disclosure and Certification Form

Failure to complete all of the following information may result in a delay in obtaining a contract, lease, purchase agreement, or grant award with any Arkansas State Agency.

SUBCONTRACTOR □ Yes ☒No   SUBCONTRACTOR NAME

TAXPAYER ID NAME: Public Consulting Group, Inc.   IS THIS FOR: □ Goods? ☒ Services? □ Both?

YOUR LAST NAME: Dobbins   FIRST NAME: Mitchell   M.I.: L

ADDRESS: 621 Capitol Mall, Suite 1425

CITY: Sacramento   STATE: CA   ZIP CODE: 95814   COUNTRY: USA

AS A CONDITION OF OBTAINING, EXTENDING, AMENDING, OR RENEWING A CONTRACT, LEASE, PURCHASE AGREEMENT, OR GRANT AWARD WITH ANY ARKANSAS STATE AGENCY, THE FOLLOWING INFORMATION MUST BE DISCLOSED:

For Individuals*

Indicate below if: you, your spouse or the brother, sister, parent, or child of you or your spouse is a current or former: member of the General Assembly, Constitutional Officer, State Board or Commission Member, or State Employee:

Position Held	Mark (√)		Name of Position of Job Held [senator, representative, name of board/ commission, data entry, etc.]	For How Long?		What is the person(s) name and how are they related to you? [i.e., Jane Q. Public, spouse, John Q. Public, Jr., child, etc.]	
	Current	Former		From MM/YY	To MM/YY	Person's Name(s)	Relation
General Assembly							
Constitutional Officer							
State Board or Commission Member							
State Employee							

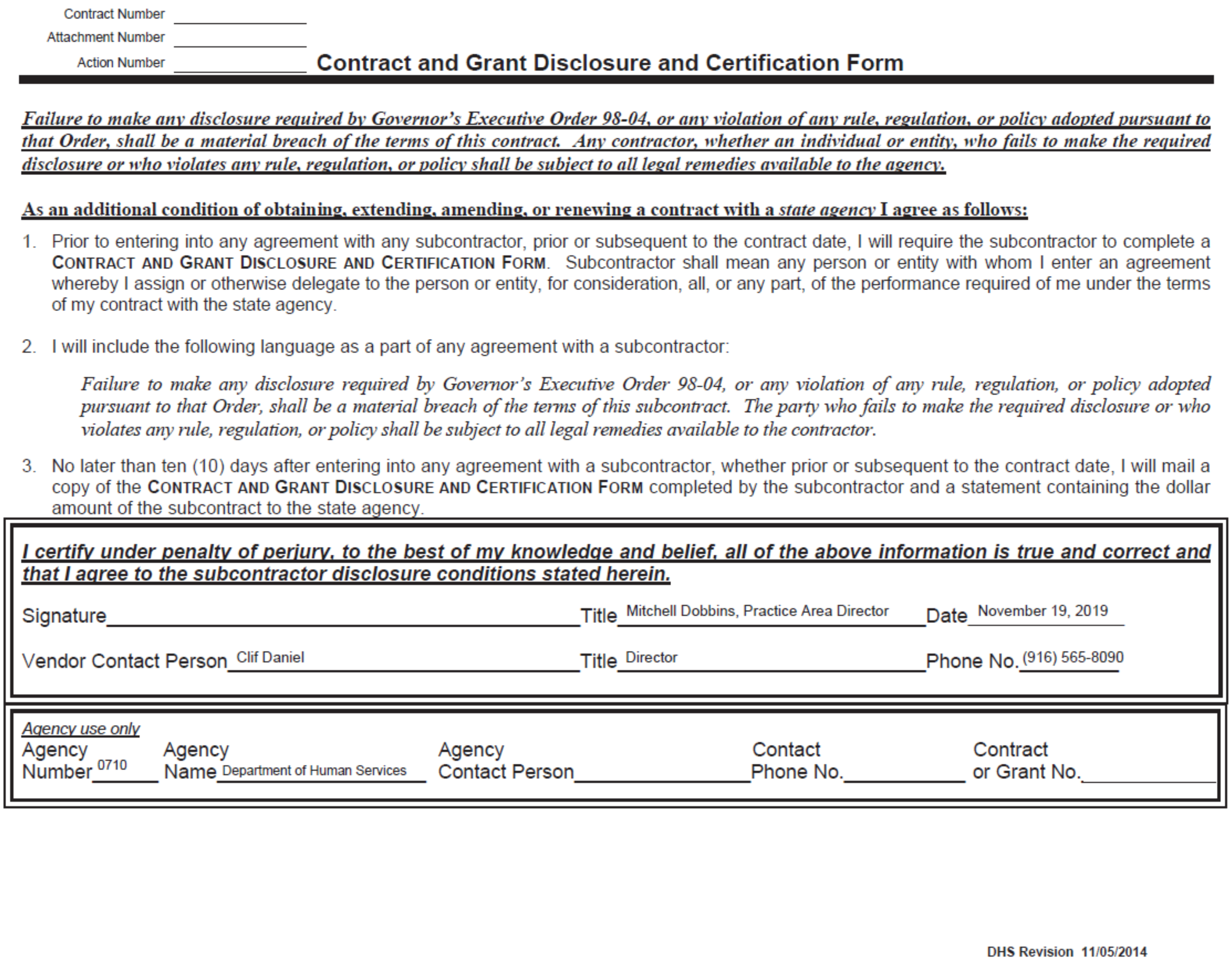
⊡ None of the above applies

For an Entity (Business)*

Indicate below if any of the following persons, current or former, hold any position of control or hold any ownership interest of 10% or greater in the entity: member of the General Assembly, Constitutional Officer, State Board or Commission Member, State Employee, or the spouse, brother, sister, parent, or child of a member of the General Assembly, Constitutional Officer, State Board or Commission Member, or State Employee. Position of control means the power to direct the purchasing policies or influence the management of the entity.

Position Held	Mark (√)		Name of Position of Job Held [senator, representative, name of board/commission, data entry, etc.]	For How Long?		What is the person(s) name and what is his/her % of ownership interest and/or what is his/her position of control?		
	Current	Former		From MM/YY	To MM/YY	Person's Name(s)	Ownership Interest (%)	Position of Control
General Assembly								
Constitutional Officer								
State Board or Commission Member								
State Employee								

⊡ None of the above applies



Contract Number ____________
Attachment Number ____________
Action Number ____________

Contract and Grant Disclosure and Certification Form

<u>Failure to make any disclosure required by Governor's Executive Order 98-04, or any violation of any rule, regulation, or policy adopted pursuant to that Order, shall be a material breach of the terms of this contract. Any contractor, whether an individual or entity, who fails to make the required disclosure or who violates any rule, regulation, or policy shall be subject to all legal remedies available to the agency.</u>

<u>As an additional condition of obtaining, extending, amending, or renewing a contract with a *state agency* I agree as follows:</u>

1. Prior to entering into any agreement with any subcontractor, prior or subsequent to the contract date, I will require the subcontractor to complete a **CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM**. Subcontractor shall mean any person or entity with whom I enter an agreement whereby I assign or otherwise delegate to the person or entity, for consideration, all, or any part, of the performance required of me under the terms of my contract with the state agency.

2. I will include the following language as a part of any agreement with a subcontractor:

   Failure to make any disclosure required by Governor's Executive Order 98-04, or any violation of any rule, regulation, or policy adopted pursuant to that Order, shall be a material breach of the terms of this subcontract. The party who fails to make the required disclosure or who violates any rule, regulation, or policy shall be subject to all legal remedies available to the contractor.

3. No later than ten (10) days after entering into any agreement with a subcontractor, whether prior or subsequent to the contract date, I will mail a copy of the **CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM** completed by the subcontractor and a statement containing the dollar amount of the subcontract to the state agency.

<u>I certify under penalty of perjury, to the best of my knowledge and belief, all of the above information is true and correct and that I agree to the subcontractor disclosure conditions stated herein.</u>

Signature ____________ Title Mitchell Dobbins, Practice Area Director Date November 19, 2019

Vendor Contact Person Clif Daniel Title Director Phone No. (916) 565-8090

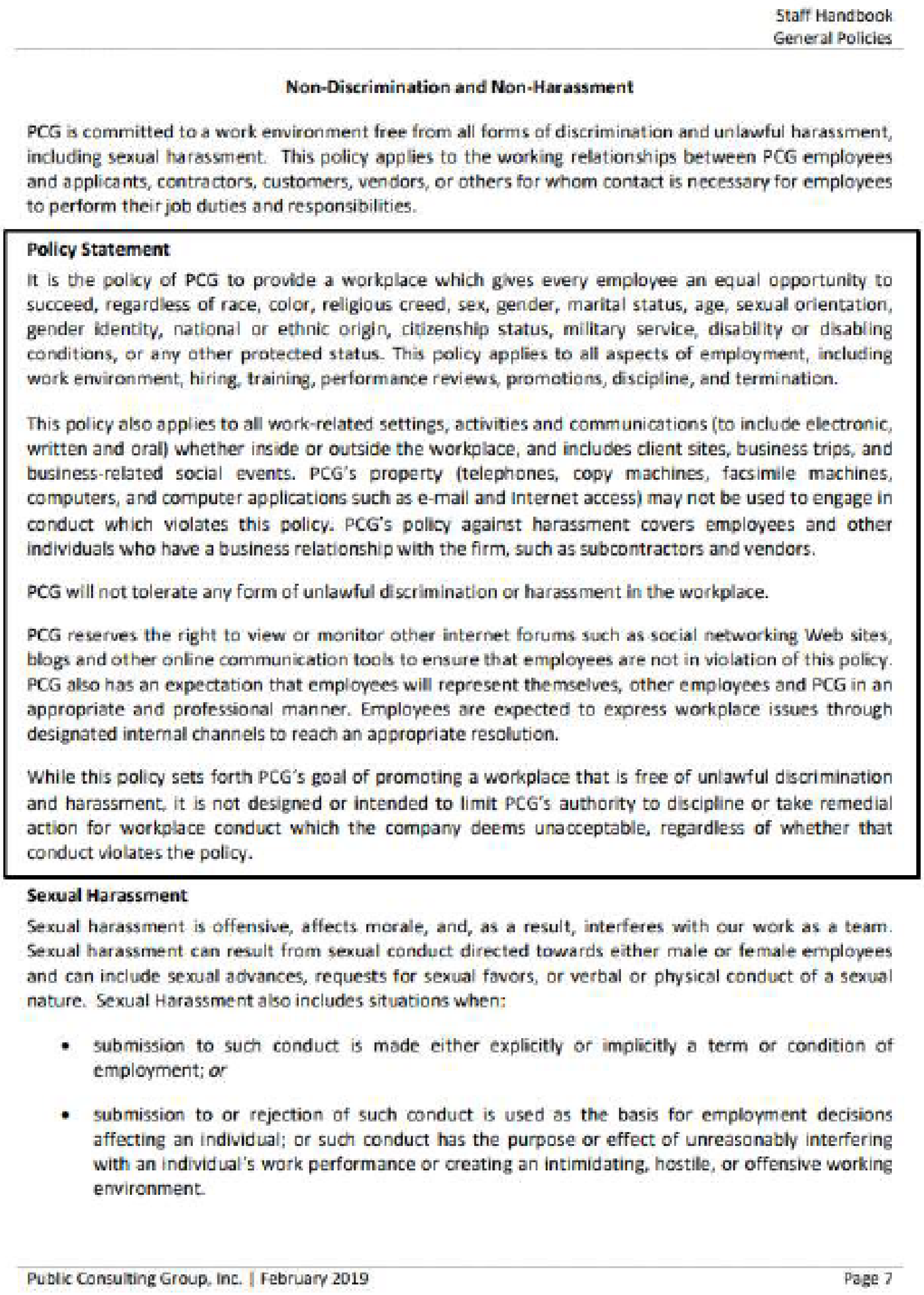
<u>Agency use only</u>

Agency Number 0710 Agency Name Department of Human Services Agency Contact Person ____________ Contact Phone No. ____________ Contract or Grant No. ____________

DHS Revision 11/05/2014

VENDOR'S EQUAL OPPORTUNITY POLICY

PCG EQUAL OPPORTUNITY POLICY



Staff Handbook
General Policies

Non-Discrimination and Non-Harassment

PCG is committed to a work environment free from all forms of discrimination and unlawful harassment, including sexual harassment. This policy applies to the working relationships between PCG employees and applicants, contractors, customers, vendors, or others for whom contact is necessary for employees to perform their job duties and responsibilities.

Policy Statement

It is the policy of PCG to provide a workplace which gives every employee an equal opportunity to succeed, regardless of race, color, religious creed, sex, gender, marital status, age, sexual orientation, gender identity, national or ethnic origin, citizenship status, military service, disability or disabling conditions, or any other protected status. This policy applies to all aspects of employment, including work environment, hiring, training, performance reviews, promotions, discipline, and termination.

This policy also applies to all work-related settings, activities and communications (to include electronic, written and oral) whether inside or outside the workplace, and includes client sites, business trips, and business-related social events. PCG's property (telephones, copy machines, facsimile machines, computers, and computer applications such as e-mail and Internet access) may not be used to engage in conduct which violates this policy. PCG's policy against harassment covers employees and other individuals who have a business relationship with the firm, such as subcontractors and vendors.

PCG will not tolerate any form of unlawful discrimination or harassment in the workplace.

PCG reserves the right to view or monitor other internet forums such as social networking Web sites, blogs and other online communication tools to ensure that employees are not in violation of this policy. PCG also has an expectation that employees will represent themselves, other employees and PCG in an appropriate and professional manner. Employees are expected to express workplace issues through designated internal channels to reach an appropriate resolution.

While this policy sets forth PCG's goal of promoting a workplace that is free of unlawful discrimination and harassment, it is not designed or intended to limit PCG's authority to discipline or take remedial action for workplace conduct which the company deems unacceptable, regardless of whether that conduct violates the policy.

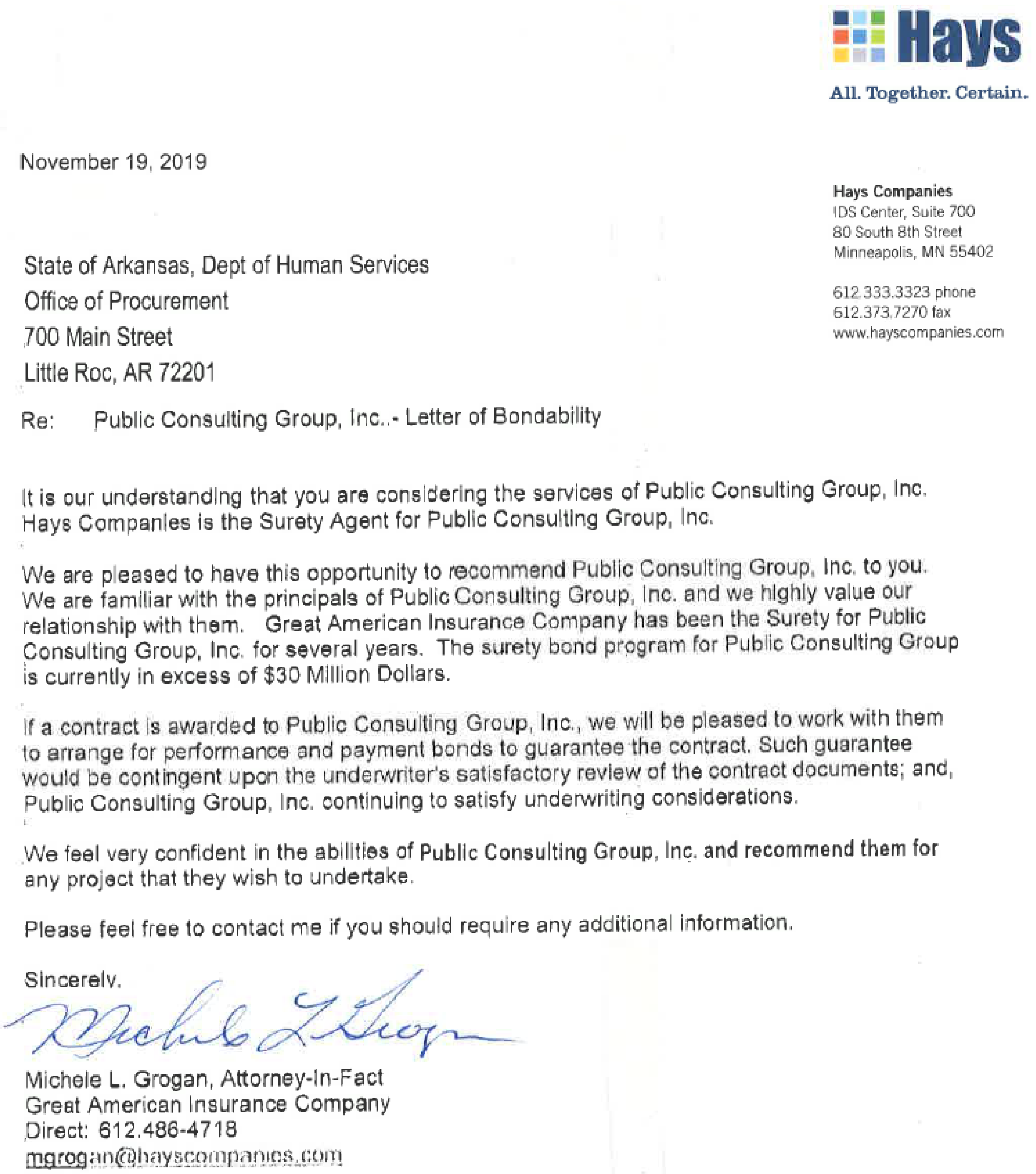
Sexual Harassment

Sexual harassment is offensive, affects morale, and, as a result, interferes with our work as a team. Sexual harassment can result from sexual conduct directed towards either male or female employees and can include sexual advances, requests for sexual favors, or verbal or physical conduct of a sexual nature. Sexual Harassment also includes situations when:

- submission to such conduct is made either explicitly or implicitly a term or condition of employment; *or*
- submission to or rejection of such conduct is used as the basis for employment decisions affecting an individual; or such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.

Public Consulting Group, Inc. | February 2019 Page 7

LETTER OF BONDABILITY



All. Together. Certain.

November 19, 2019

Hays Companies
IDS Center, Suite 700
80 South 8th Street
Minneapolis, MN 55402

612.333.3323 phone
612.373.7270 fax
www.hayscompanies.com

State of Arkansas, Dept of Human Services
Office of Procurement
700 Main Street
Little Roc, AR 72201

Re: Public Consulting Group, Inc..- Letter of Bondability

It is our understanding that you are considering the services of Public Consulting Group, Inc. Hays Companies is the Surety Agent for Public Consulting Group, Inc.

We are pleased to have this opportunity to recommend Public Consulting Group, Inc. to you. We are familiar with the principals of Public Consulting Group, Inc. and we highly value our relationship with them. Great American Insurance Company has been the Surety for Public Consulting Group, Inc. for several years. The surety bond program for Public Consulting Group is currently in excess of $30 Million Dollars.

If a contract is awarded to Public Consulting Group, Inc., we will be pleased to work with them to arrange for performance and payment bonds to guarantee the contract. Such guarantee would be contingent upon the underwriter's satisfactory review of the contract documents; and, Public Consulting Group, Inc. continuing to satisfy underwriting considerations.

We feel very confident in the abilities of Public Consulting Group, Inc. and recommend them for any project that they wish to undertake.

Please feel free to contact me if you should require any additional information.

Sincerely,

Michele L Grogan

Michele L. Grogan, Attorney-In-Fact
Great American Insurance Company
Direct: 612.486-4718
mgrogan@hayscompanies.com

INDEPENDENT AUDITED FINANCIAL STATEMENT

PCG's independent audited financial statement is provided beginning on the next page.

Subject: Confidential Audited Financial Statements

Dear Ladies and Gentlemen:

WARNING

The attached Audited Financial Statements for Public Consulting Group, Inc. (PCG) are proprietary and confidential. The Statements contain a CONFIDENTIAL watermark and are accessible on a limited and controlled basis. If they are made available to anyone except the government agency that has specifically requested them, sensitive and confidential PCG business information could become available to PCG competitors and partner companies and provide them with an unfair competitive advantage. To avoid any such risk, we ask that you comply with the following safeguards:

1. Print out and distribute only the minimum number of copies that you need to fulfill the request.
2. Immediately shred all additional hard copies of the document(s).
3. Immediately delete the document from the files that you store electronically, and
4. Do not distribute the electronic document to anyone else, either internally or externally.

For control purposes, access to the statements is managed through a log maintained by the PCG Finance Department.

If you have questions about these required steps, please contact PCG Vice President of Finance Rolf Ruben.

PROPOSAL

INTRODUCTION

Public Consulting Group, Inc. (PCG) is pleased to present our proposal to provide Minimum Acceptable Risk Standards for Exchanges (MARS-E 2.0) Independent Security Assessment services to support the Arkansas Department of Human Services project to replace its current eligibility and enrollment system with the of the Integrated Eligibility and Benefit Management Solution (IEBM) called the Arkansas Integrated Eligibility System (ARIES). PCG's services will be provided to satisfy the Centers for Medicare and Medicaid Services (CMS) rules regarding the State's Authority to Connect (ATC) to the Federal Data Services Hub as well as their security control attestation requirements.

PCG has conducted MARS-E independent security assessments since 2013, adhering to CMS requirements. Additionally, PCG has experience using the National Institute of Standards Technology (NIST) Special Publication 800 series guidance, and the MARS-E source framework, for over 12 years. PCG has worked with Deloitte previously with the NextGen system. PCG has recently worked with Deloitte and the NextGen system in multiple states in the eastern United States, including Louisiana, Georgia, Delaware, and Tennessee.

Our proposed security staff have provided security expertise over the years in both public, and private sector business verticals, including health care systems in the capacity of enterprise project management, independent verification and validation (IV&V), and security controls assessments for CMS and integrated eligibility systems. To ensure a high quality assessment, the PCG security team is well versed in the application of applicable federal, state, and local laws as well as Health Information Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH), and IRS Publication 1075 and uses the information for guidance in assessing appropriate security and privacy measures.

PCG recognizes that performing independent security and privacy assessments is not just the act of "checking the boxes" to complete a federal requirement. PCG goes beyond checking boxes by informing our clients of security risks within the system that should be mitigated. Security assessments are intended to identify gaps in the security and privacy of a system needed to maintain confidentiality, integrity, and availability. Our team will thoroughly review the documents, artifacts, and other evidence to ensure that the implementation standards of MARS-E standards are met or exceeded. If the documentation or evidence provided does not provide enough information to satisfy MARS-E implementation standards, the PCG team will seek additional information through interviews to determine the implementation state of specific controls or control enhancements. The PCG team has worked in many other states on their integrated eligibility systems that support the following government programs:

- Child Support Enforcement (CSE)
- Childcare Assistance
- Children's Health Insurance Programs (CHIP)
- Comprehensive Child Welfare Information System (CCWIS)
- Low Income Home Energy Assistance Programs (LIHEAP)
- Medicaid (traditional and MAGI)
- Food Stamps (SNAP)

- Temporary Assistance for Needy Families (TANF)
- Veteran’s Services
- Women, Infants, and Children (WIC & eWIC)
- Law Enforcement (CJIS)

Assessment Plan

PCG’s independent security assessments validate that all necessary security controls are integrated into the design and implementation of a solution, and where applicable, identify any security gaps between system security controls and approved security policies governing an agency or organization. PCG’s experience delivering MARS-E assessments will guide the development of our assessment plan to achieve successful completion.

Our independent security assessments conform to the Independent Assessment of Security and Privacy Controls framework released by CMS in March 2016, which provides guidance and direction for assessments of MARS-E v2.0 security and privacy controls.

Our independent security assessment services are modeled by NIST Special Publication 800-53 R4 - Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800-53A R4- Guide for Assessing the Security Controls in Federal Information Systems and Organizations. We use the NIST Risk Management Framework (RMF), which has been configured to public sector information security needs, as guided by FIPS Publication 199 - Security Categorization of Federal Information Systems. Key artifacts of the RMF include:

- NIST Special Publication 800-39, Managing Information Security Risk – Organization, Mission, and Information System View
- NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments
- NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST Special Publication 800-53A Revision 4, Guide for Assessing Security Controls in Federal Information Systems

To perform independent security assessments per the NIST 800-53A Revision 4 and CMS control guidelines, we examine organization and project artifacts, such as System Security Plan (SSP), conduct site visits and interviews, perform security tests and review security policies and procedures. Assessment objectives are used to determine security control accuracy, completeness, and maintainability to support the continuous monitoring necessary, and can be used to mature an organization’s information security program.

The NIST-defined assessment procedure provides a standardized approach for scoping, planning, performing, documenting, and managing an information security assessment. An information security assessment is a process of determining how effectively an entity, such as a host, system, network, procedure, person (known as the assessment object), meets specific information security assessment objectives.

PCG uses three methods to conduct the security and privacy controls assessments, as displayed in Table 1 and depicted in the following sections.

Table 1: Independent Security Assessment Methods

PCG Assessment Methods			
#	**Method**	**Description**	**Examples**
1	**Examination**	The examination is the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objectives to facilitate understanding, achieve clarification, or obtain evidence.	• Document Review • Observation
2	**Interviewing**	Interviewing is the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or identify the location of evidence. Auditing activities are generally reviewed as part of interviews, due to access and the sensitive nature of data.	• On-site/In-person • Phone Interviews
3	**Testing**	Testing is the process of exercising one or more assessment objectives under specified conditions to compare actual and expected behaviors. Testing can be carried out by directly accessing and manipulating the target objective and analyzing the results against expectations, or it can be done by comparing the output of regular functions to regulatory frameworks or industry standards.	• Security Control Technical Testing • Network and Component Scanning

Method 1 – Examination

Two forms of examination support the Security Assessment Report (SAR) activities:

- Document review
- Observation

Examination Approach #1 – Document Review

Document review is the process of inspecting, reviewing, and analyzing documents to facilitate understanding, achieve clarification, or obtain evidence for one or more assessment objectives. Our team starts with a review of the MARS-E System SSP. The SSP is the single artifact that ensures that controls are in place and documented or identified as deficiencies with the corresponding remediation action plans. The SSP is the most critical input into any assessment of risk of a system. We will perform a thorough examination of security and privacy documentation, including all core security and privacy documents provided by Arkansas DHS. To guide our data collection activities, PCG will provide our MARS-E Assessment Preparation Guide that leverages our experience with the MARS-E assessment process to facilitate artifact discovery and analysis. This guide identifies security control assessment documents, such as the SSP and the Plan of Actions and Milestones (POA&M), to be provided at the onset of the project to quickly ramp up assessment activities. Table 2 on the next page identifies the core MARS-E documentation required in the CMS System Certification Authority to Operate (ATO) Request Form. The review of this documentation is critical to a successful security assessment of Medicaid and Integrated Eligibility systems.

Table 2: MARS-E v2.0 Core Documentation for ATO

MARS-E v2.0 Control Family	MARS-E v2.0 Control Number	Document Name
Security and Assessment Authorization (CA)	CA-2: Security Assessments	• Security Control Assessment (SCA) Plan • SCA Report
Security and Assessment Authorization (CA)	CA-3: System Interconnections	• Interconnection Security Agreement(s) (ISA) • Memorandum(s) of Agreement/Understanding (MOA/U) • Service Level Agreement (SLA)
Security and Assessment Authorization (CA)	CA-5: Plan of Action and Milestones	• POA&M
Contingency Planning (CP)	CP-2: Contingency Plan	• Contingency Plan (CP)
Contingency Planning (CP)	CP-4: Contingency Plan Testing and Exercises	• CP Test Plan • Current CP Test After Action Report
Planning (PL)	PL-2: Security System Plan	• SSP
Risk Assessment (RA)	RA-3: Risk Assessment	• Information Security Risk Assessment (ISRA)
Authority and Purpose (AP)	AP-1: Authority to Collect	• Privacy Impact Assessment (PIA)

PCG's previous experience allows us to identify typical documentation received from state agencies to help ensure a quick start to assessment of the Arkansas Integrated Eligibility System. Table 3 lists some of the standard documentation needed to meet MARS-E control requirements that are created and maintained by the state agency and supporting vendors.

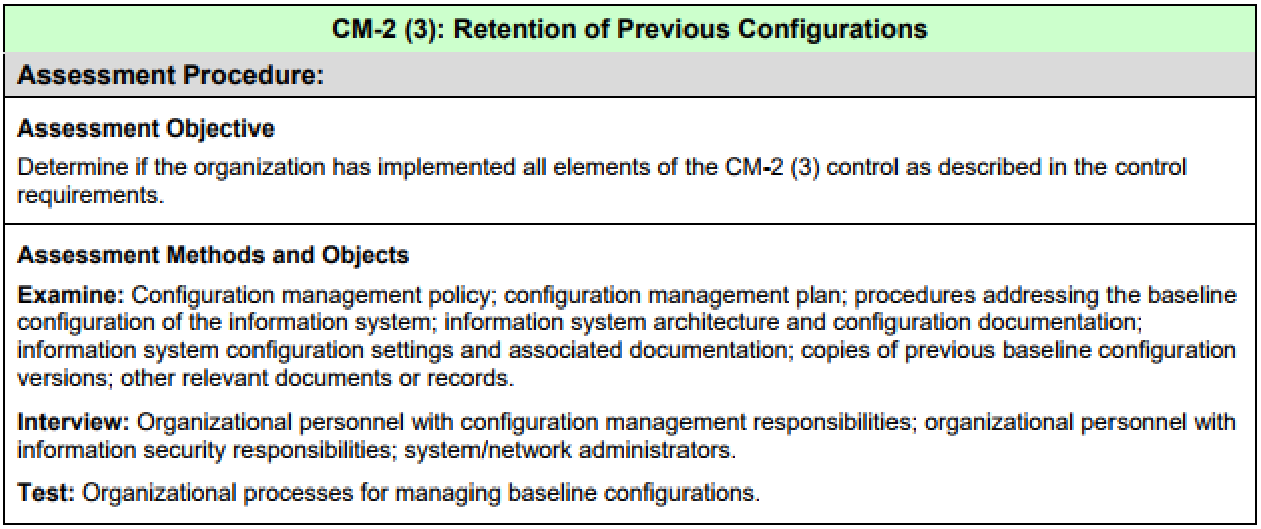
Table 3: MARS-E Preparation Guide Inputs

MARS-E v2.0 Control Family	Documents Required
Access Control (AC)	• Access Control Policy and Procedures • Identity and Access Management Plan • System Roles and Responsibilities Matrix
Audit and Accountability (AU)	• Audit Policy and Procedures • Capacity Management Plan • Audit Sources • Auditable Events
Awareness and Training (AT)	• Security Awareness and Training Policy and Procedures • Security and Privacy Awareness and Training Plan (required artifact)

MARS-E v2.0 Control Family	Documents Required
	• Security and Privacy Training Guides and Records
Configuration Management (CM)	• Configuration Management Policy and Procedures • Configuration Management Plan (required artifact) • Change Management Plan • Configuration Change Control Records • Security Impact Analysis
Contingency Planning (CP)	• Contingency Planning Policy and Procedures • Business Continuity Plan • Disaster Recovery Plan • Disaster Recovery Test Plan • Most Recent Disaster Recovery Test Report • Disaster Recovery Test Results • Alternate/Primary Storage Site Agreements
Identification and Authentication (IA)	• Identification and Authentication Policies and Procedures
Incident Response (IR)	• Incident Response Policy and Procedures • Incident Response Plan (required artifact) • Incident Response Training Materials • Incident Response Test Plan • Incident Response Test Results
Maintenance (MA)	• Maintenance Policy and Procedures
Media Protection (MP)	• Media Protection Policy and Procedures
Personnel Security (PS)	• Personnel Security Policy and Procedures
Physical and Environmental Protection (PE)	• Physical and Environmental Protection Policy and Procedures • Physical Security Plan
Planning (PL)	• Information Security Planning Policy and Procedures • Information Security Program Plan • Security Metrics Program • Security Monitoring Plan
Risk Assessment (RA)	• Risk Assessment Policy and Procedures • Risk Assessment Reports • Vulnerability Management Plan • Vulnerability Scan Report • Security Assessment Reports
System and Services Acquisition (SA)	• System and Services Acquisition Policy and Procedures • System and Service Acquisition Documents
System and Communications Protection (SC)	• System and Communications Protection Policy and Procedures • Network Architecture Documentation
System and Information Integrity (SI)	• System and Information Integrity Policy and Procedures • System Architecture Documentation • System Design Documentation
Program Management (PM)	• Information Security Program Plan • Threat Management Plan

MARS-E v2.0 Control Family	Documents Required
	• Organization Charts • Threat Management Plan
Authority and Purpose (AP)	• System of Records Notice (SORN) • Privacy Act Statement • Computer Matching Agreement (CMA) • Information Exchange Agreements (IEA) • Privacy documents and notices including agreements to collect, use, and disclose Personally Identifiable Information (PII)
Accountability, Audit, and Risk Management (AR)	• Privacy Plan • Privacy Policies • Governance documents • Documentation describing the Administering Entity (AE) privacy risk assessment process, documentation of privacy risk assessments performed by the organization
Data Quality and Integrity (DI)	• Data Quality Procedures
Data Minimization and Retention (DM)	• PII Retention Policy • PII holding evaluation and review documentation • PII Disposal Procedures
Security (SE)	• Privacy Incident Response Plan • PII Inventory
Use Limitation (UL)	• Data Matching and Sharing Agreements

Target assessment objectives are often overlapping because of their dependence on reference artifacts that are primarily required and addressed by other controls. These overlapping objectives are deferred to their parent, or source controls for examination and do not need to be referenced. For example, Figure 1 denotes a notation for CM-E(s) – Retention of Previous Configurations requiring that organizations define and maintain configuration baselines of information systems. The control requires examination of configuration management policy and procedures, which are defined by CM-1 and examination of the configuration management plan, defined by CM-9. CM-2(3) does not need to include references to policy and configuration management plans, as these will be assessed as part of their primary control.



CM-2 (3): Retention of Previous Configurations

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the CM-2 (3) control as described in the control requirements.

Assessment Methods and Objects

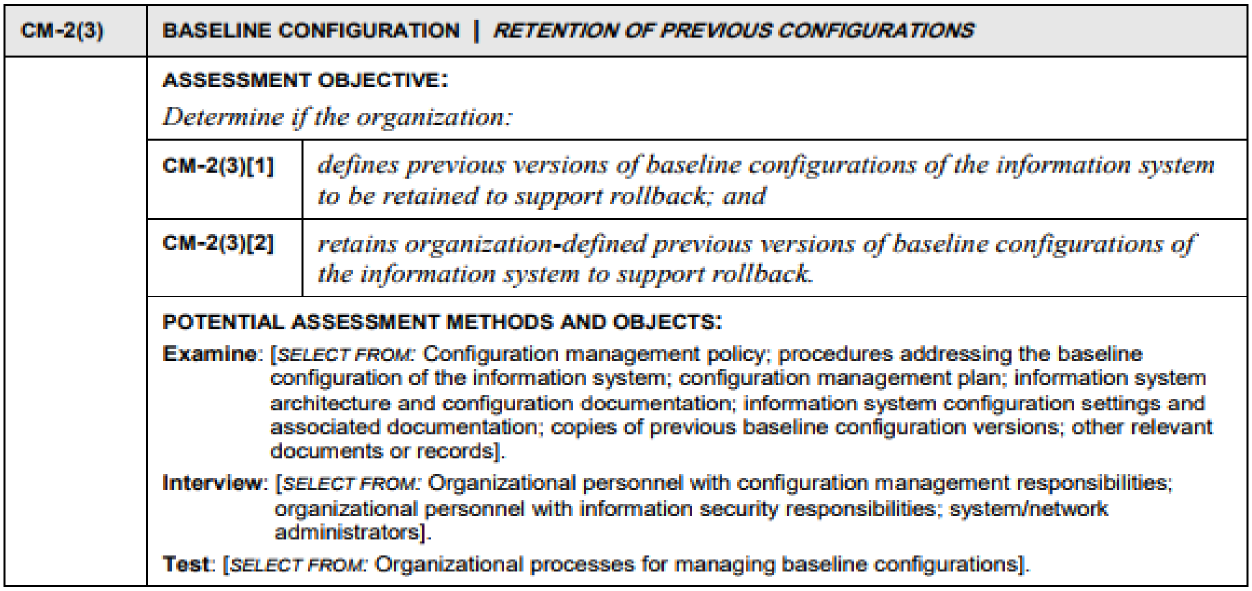
Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; information system configuration settings and associated documentation; copies of previous baseline configuration versions; other relevant documents or records.

Interview: Organizational personnel with configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for managing baseline configurations.

Figure 1: MARS-E 2.0, CM-2(3)

Further, MARS-E and NIST SP 800-53A primarily differ in that NIST (Figure 2 on the following page) identifies more granular assessment statements (CM-2(3)[1] and CM-2(3)[2]). This allows for a more nuanced assessment approach, as controls can be partially met.



CM-2(3)	**BASELINE CONFIGURATION | *RETENTION OF PREVIOUS CONFIGURATIONS***	
	ASSESSMENT OBJECTIVE: *Determine if the organization:*	
	CM-2(3)[1]	*defines previous versions of baseline configurations of the information system to be retained to support rollback; and*
	CM-2(3)[2]	*retains organization-defined previous versions of baseline configurations of the information system to support rollback.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing the baseline configuration of the information system; configuration management plan; information system architecture and configuration documentation; information system configuration settings and associated documentation; copies of previous baseline configuration versions; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators]. **Test**: [*SELECT FROM:* Organizational processes for managing baseline configurations].	

Figure 2: NIST SP 800-53a Rev 4, CM-2(3)

We will review and assess documents against controls that may overlap or connect to security controls through parent or child relationships or inherited controls that are common throughout the enterprise. For example, the Integrated Eligibility and Benefits Management Solution may utilize a separate identity management system for the state or agency enterprise environment. In this example, the IBEM may “inherit” common controls from the identity management system. Providing enough documentation contributes to producing a more accurate representation of your system and security environment. The absence of information within documentation, evidence, and interviews may result in an assessment finding that is inaccurate.

EXAMINATION APPROACH #2 – OBSERVATION

PCG will perform observational assessments on process improvements, physical security, environmental security, and other areas of concern. These observations will be included as findings in the SAR and documented for client awareness and action. The findings may be classified as a preliminary concern, neutral finding, risk, or event.

- **Preliminary Concern –** Presents an observation of an event or condition for which insufficient factual or empirical information is available to be classified as a risk or issue, but that warrants continued observation.
- **Neutral Finding –** Does not necessarily have an impact on the project. These are general suggestions for an alternative approach.
- **Risk –** "An uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives." We identify risks with adverse effects and expand the definition to include both conditions which may occur, and those that may not happen, such as the lack of a well-defined requirements traceability process, could lead to the delivery of an incomplete system, requiring costly and time-consuming rework.
- **Event –** Often previously identified as a risk, which has been realized and caused a negative impact on the project. Issues are documented as findings that identify the event, its impact on the project, and status towards resolution.

Whenever possible, we will immediately alert the Arkansas DHS staff to risks that can be quickly mitigated before the SAR is complete and allow for re-assessment within agreed-upon milestone/cut-off dates.

Findings will be included in a Status Report, prioritized by red, yellow, and green, as shown in Table 4.

Table 4: Risk Priority and Descriptions

Risk Priority	Description
HIGH	The possibility of a substantial impact on product quality, manageability, cost, or schedule. Significant disruption is likely, and the consequences would be unacceptable. A different approach is required. Mitigation strategies should be evaluated and acted upon immediately.
MEDIUM	The possibility of a moderate impact on product quality, manageability, cost, or schedule. Some disruption is likely, and a different approach may be required. Mitigation strategies should be implemented as soon as feasible.
LOW	The possibility of a slight impact on product quality, manageability, cost, or schedule. Minimal disruption is likely, and some oversight is needed to ensure that the risk remains low. Mitigation strategies should be considered for implementation when possible.

Method 2 – Interviewing

Our second method of security assessment is to validate the implementation standard throughout your organization by interviewing your stakeholders and administrative personnel. Our security team will require support from the Arkansas DHS staff via scheduled meetings to ensure that baseline documentation identified in MARS-E v2.0 Core Documentation for ATO and MARS-E Preparation Guide Inputs (stated above) are available. Interviews with Arkansas ARIES subject matter experts is crucial to ensuring potential findings are accurate and understood by the assessment team. Our security team will provide you with interview schedules in advance, which serves to notify key personnel of interview purpose, timing, and objectives. Roles that are expected to be interviewed include, but are not limited to:

- Chief Information Security Officer
- Chief Privacy Officer
- Information Security Officer
- System Administrator
- Security Administrator
- Change Management Lead
- Configuration Management Lead
- Disaster Recovery Lead
- Risk Manager
- Incident Response Lead
- Account Manager
- Chief Information Officer

Method 3 – Testing

Security testing is the final security assessment method we will use. Testing validates that all levels of application security have been implemented based on security requirements, design specifications, and to assess system vulnerability to external threats. Security testing occurs in the following ways:

Security Control Technical Testing

PCG will either directly conduct security testing activities against the system or will guide the Arkansas Department of Human Services system staff in performing technical tests that our assessors then validate to verify that controls are adequately implemented. This flexibility will allow DHS to establish their level of comfort with how security testing activities are performed.

Network and Component Scanning

Like Security Control Technical Testing, our role is to determine which tools will yield the desired results and validate configurations of components if not already in place and configured. If necessary, our assessment team will guide the DHS system or vendor staff on the required results from testing to ensure compliance with MARS-E standards. If your system does not have the scanning capability in place for discovering ports, protocols, and services running, we will recommend the appropriate tools or scripts for potential agency deployment.

Configuration Assessment

PCG will compare system and application configurations to requirements and best practices, such as the Center for Internet Security (CIS) Benchmarks, NIST standards, and vendor-specific tools and checklists. Other tasks performed include review access rights to configuration items and firewall rules.

Vulnerability Identification

As required by MARS-E Control RA-5, PCG will work with the ARIES team to obtain detailed vulnerability/compliance scan reports, port scanning, and penetration testing results as part of the assessment process of the ARIES system.

MINIMUM QUALIFICATIONS

VENDOR QUALIFICATIONS

Project 1: Delaware Department of Health and Social Services

Application for Social Services and Internet Screening Tool (ASSIST) Assessment

TIME PERIOD July 2017 – April 2018 **PROJECT AMOUNT** $ 110,000

DESCRIPTION OF WORK:

In addition to IV&V services, PCG provided an independent SCA for the Department's ASSIST system based on the CMS MARS-E 2.0 framework. PCG performed a MARS-E v2.0 assessment on the Deloitte NextGen eligibility system for the fiscal year 2017. Delaware had an active ATC to the Federal Data Services Hub for a period of three years is active, and security team assessment encompassed an examination of an annual subset of controls. The assessment verified that the documented security controls had been completed (per the system design), and any identified security risks (if any existed) were mitigated. Besides the MARS-E 2.0, the team also used guidance from:

- NIST Special Publications: 800-53A, 800-30 and 800-37
- IRS Publication 1075

Project 2: Hawaii Department of Human Services

Kauhale On-Line Eligibility Assistance (KOLEA) Independent Assessment of Security and Privacy Controls

TIME PERIOD January 2013 – Present **PROJECT AMOUNT** $ 747,000

DESCRIPTION OF WORK:

PCG has provided independent security services for the Hawaii Department of Human Services since 2013. Starting in 2013, the agency replaced its legacy Medicaid eligibility system with a commercial off-the-shelf (COTS) solution to modernize its system and support the ACA requirements. The KOLEA project was multi-phased with a first release that went live on October 1, 2013. The initial release converted all the Medicaid functionality from the legacy system to KOLEA and creating a Department enterprise platform to first support the benefits, employment and support services programs such as SNAP, TANF, and LIHEAP, followed by social services programs including child welfare, adult protective services, and others to offer well-coordinated holistic consumer services. These initiatives were analogous to being "modular" in that the designed enterprise platform, which was managed by the enterprise system integrator (ESI) provider, hosted multiple applications. As part of our long-standing assistance with the KOLEA system in Hawaii, PCG has conducted various independent security control assessments of Hawaii's modernized eligibility and enrollment system since 2013 through present day. Our assessments have included external vulnerability testing and penetration testing in addition to the MARS-E v2.0 and v1.0. Assessments included:

- MARS-E v2.0 independent security assessment
- Annual attestations for MARS-E v1.0 & 2.0
- Additional security services throughout multiple engagements have included:
    - Penetration and vulnerability testing
    - HITRUST gap analysis
    - Development of privacy and security policies for the agency

KEY PERSONNEL RESUMES

The PCG assessment team proposes the following staff, including a Lead Assessor, that will be dedicated during the ARIES assessment activities. Additionally, we propose two additional security and privacy subject matter experts (SME) that will be used on an as-needed basis.

Our proposed SMEs have additional technical experience, specifically with the Deloitte NextGen system, and systems that focus on the usage of confidential data in Health and Human Service systems, including but not limited to federal tax information, criminal justice information, and technical experience in cloud and datacenter technology.

Manuel (Manny) Barandas, Senior Consultant

Lead Assessor

Relevant Qualifications
Minimum of three (3) years of SCA experience: Manny has three years and six months of experience performing the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Must show past SCA work on at least one (1) eligibility engagement that supported a state Medicaid system: Manny has performed SCA work on three eligibility engagements that supported state Medicaid systems in Delaware, Iowa and Hawaii.
Security and Privacy certifications: Manny has the following security and privacy certifications: • Microsoft Certified Solutions Expert (MCSE), specializing in Securing Windows Server 2016 • CompTIA Cybersecurity Analyst+ (CySA+), June 2018 • CompTIA Security Analytics Professional (CSAP), June 2018 • Certified Information Systems Security Specialist (CISSP), April 2015 • Tenable Certified Nessus Auditor, January 2015 • CompTIA Security+, July 2012
Experience developing security project plans: Manny developed security project plans for the MARS-E Assessment with the state of Hawaii, including status reports delivery, state resource requirements & working with stakeholders on report drafts, reviews and submission
Deloitte NextGen experience: Manny worked with Deloitte as a team member on the IV&V vendor team during the Michigan BRIDGES modernization project. Manny is also an IBM Certified Associate Business Process Analyst for Cúram.

Relevant Project Experience

Hawaii Department of Human Services

Medicaid Eligibility System, Kauhale On-Line Eligibility Assistance (KOLEA)

MARS-E Lead Security Analyst | July 2018 – August 2019

Manny served as the MARS-E Technical Lead conducting an independent assessment of security and privacy controls for the Department's Enterprise Program to meet federal requirements, including all the requirements of the CMS Framework for the Independent Assessment of Security and Privacy Controls Version 2.0 Final. Work included a complete assessment of all MARS-E security controls, penetration testing, and an annual security control attestation. This work utilized MARS-E 2.0 along with NIST 800-53A as guidance.

Manny's responsibilities included:

- Provided MARS-E Assessment Guide that included identifying state resource requirements
- Audited KOLEA security controls against MARS-E 2.0 and supplemental requirements
- Assessed technical controls at the application, system and network levels
- Aggregated results to determine project security risks, managing the security team, authoring the report, and working with stakeholders on report drafts, reviews, and submission

- Developed weekly status reports on resource and project status, accomplishments, risks, issues, and concerns

PROJECT REFERENCE			
NAME	Lim Yong	TELEPHONE	808-692-8071
PROJECT ROLE	Privacy Officer		

Iowa Department of Human Services, Medicaid Eligibility System

Medicaid Eligibility System, Eligibility Integrated Application Solution (ELIAS)

MARS-E Security Analyst | February 2018 – May 2018

PCG provided a 2nd annual independent Security Control Assessment to verify that the ELIAS system is properly implementing information security. PCG used the NIST-based MARS-E 2.0 to validate processes and configurations, review security documentation, and conduct interviews. The assessment verified that the documented security controls complied with the system design, and any security risks were mitigated. The scope of the assessment was MARS-E 2.0 Year 1 Security Controls and provided CMS security control results.

Manny’s responsibilities included:

- Audited ELIAS security controls against MARS-E 2.0 and supplemental requirements
- Reviewed information security documentation
- Assessed technical controls at the application, system, and network levels

PROJECT REFERENCE			
NAME	Brenda Hall	TELEPHONE	515-725-1340
PROJECT ROLE	Contract Manager		

Delaware Department of Health and Social Services

Medicaid Eligibility System, Application for Social Services Internet Screening Tool (ASSIST)

MARS-E Security Analyst | November 2017 – February 2018

PCG provided an independent Security Control Assessment to verify the ASSIST system complied with the CMS MARS-E 2.0 framework information security requirements. PCG used the NIST-based MARS-E 2.0 to validate processes and configurations, review security documentation, and conduct interviews. The assessment verified that the documented security controls had been completed (in accordance with the system design), and any identified security risks (if any existed) were mitigated. The scope of the assessment was a full assessment of MARS-E 2.0 security controls.

Manny’s responsibilities included:

- Audited ELIAS security controls against MARS-E 2.0 and supplemental requirements
- Reviewed information security documentation
- Assessed technical controls at the application, system, and network levels

PROJECT REFERENCE			
NAME	Michael A. Smith	TELEPHONE	302-255-9162
PROJECT ROLE	Applications Director		

Iowa Department of Human Services

Medicaid Eligibility System, Eligibility Integrated Application Solution (ELIAS)

MARS-E Security Analyst | April 2017 – July 2017

PCG provided an independent Security Control Assessment to verify that the ELIAS system is properly implementing information security. PCG used the NIST-based MARS-E 2.0 to validate processes and configurations, review security documentation, and conduct interviews. The assessment verified that the documented security controls had been completed (in accordance with the system design), and risks (if any existed) were mitigated. The scope of the assessment was a full assessment of MARS-E 2.0 security controls.

Manny's responsibilities included:

- Auditing ELIAS security controls against MARS-E 2.0 and supplemental requirements
- Reviewing information security documentation
- Assessing technical controls at the application, system, and network levels

PROJECT REFERENCE			
NAME	Brenda Hall	TELEPHONE	515-725-1340
PROJECT ROLE	Contract Manager		

California Department of Public Health (CDPH)

Health Insurance Portability and Accountability (HIPAA) Assessment

Lead Security Analyst | March 2016 – June 2017

PCG provided an independent security and privacy assessment to ensure CDPH fulfilled the Health Insurance Portability and Accountability Act (HIPAA) risk assessment and management requirements, as well as compliance with the security controls in the California State Administrative Manual (SAM) Section 5300.

As the Lead Security Analyst, Manny conducted a comparative analysis in line with SAM Sections 5300-5399, Statewide Information Management Manual (SIMM) Section 5300, and NIST 800-53 Revision 4 Security Control Mapping.

PROJECT REFERENCE			
NAME	Charles Lano	TELEPHONE	(916) 322-2649
PROJECT ROLE	Department Chief Information Security Officer (CISO)		

ADDITIONAL EXPERIENCE

Michigan Department of Health and Human Services

MDHHS Bridges Modernization Project

IV&V Consultant | January 2018 – Present

The purpose of this project is to implement and deploy enhancements as part of the State's Bridges Modernization project. Manny's responsibilities included:

- Conducting independent verification and validation to ensure proper best practices and industry standards are being utilized during each phase of the SDLC against MITA Framework and CMS MEELC guidelines

- Attending technical, operations, and risk management meetings to identify potential risks to the success of the project
- Reviewing technical and security-related documentation
- Observing activities based on industry best practices, IEEE and NIST Standards, CMS MITA guidelines, appropriate MEELC checklists, and standards for CMS Certification
- Writing CMS progress reports in preparation for state and CMS delivery
- Assessed and analyzed project planning documents, which included:
  - Disaster Recovery Plan
  - Contingency Plan

PROJECT REFERENCE			
NAME	Brant Cole	TELEPHONE	(517) 241-0288
PROJECT ROLE	Director		

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- CompTIA Security Analytics Professional
- CompTIA Security Analytics Professional
- CompTIA Security+
- CompTIA Network+
- CompTIA A+
- Information Technology Infrastructure Library (ITIL) v3 Foundation
- IBM Certified Associate Business Process Analyst
- Tenable Certified Nessus Auditor
- Tenable Certified Nessus User

MICROSOFT CERTIFICATIONS

- Microsoft Certified Solutions Expert (MCSE): Core Infrastructure
- Microsoft Certified Solutions Associate (MCSA): Windows Server 2012
- Microsoft Certified Solutions Associate (MCSA): Windows Server 2008
- Microsoft Certified IT Professional (MCITP) 2008: Server Administrator on Windows Server 2008
- Microsoft Certified Technology Specialist (MCTS): Windows Server 2008 Network Configuration
- Microsoft Certified Technology Specialist (MCTS): Windows Server 2008 Active Directory
- Microsoft Certified Systems Engineer (MCSE): Security on Windows Server 2003
- Microsoft Certified Systems Engineer (MCSE): Windows Server 2003
- Microsoft Certified Systems Administrator (MCSA): Messaging on Windows Server 2003
- Microsoft Certified Systems Administrator (MCSA): Windows Server 2003
- Microsoft Certified Systems Administrator (MCSA): Windows Server 2000
- Microsoft Certified Professional (MCP)

TRAINING/SKILLS

- Pentest with Hak5
- New Horizons Computer Center
- TechSkills

Jeff Neithercutt, Senior Information Security Consultant

Security & Privacy SME

Relevant Qualifications
Minimum of three (3) years of SCA experience: Jeff has a total of eight years and two months of SCA experience.
Must show past SCA work on at least one (1) eligibility engagement that supported a state Medicaid system: Jeff is the PROJECT ROLE on the Mississippi Department of Medicaid Modularized MES project.
Security and Privacy certifications: Jeff possesses the following security and privacy certifications: • CISSP • CompTIA CySA+ • National Security Agency NSTISSI 4011 National Training • Standard for Information Security Systems Professional • National Security NSTISSI 4012 National • Information Assurance Training Standard for Senior Systems Managers • TLO Advanced Course: Cyber Security-High Technology Threats
Experience developing security project plans: Jeff has over two years of experience developing security project plans for California Child Welfare Digital Services (CWDS), California Department of Justice, and San Francisco Department of Public Health (SFDPH).

Relevant Project Experience

Mississippi Department of Medicaid (DOM)

Modularized Medicaid Enterprise System

IV&V Security SME | September 2019 – Present

Jeff is the IV&V Security and Disaster Recovery SME DOM's project to replace its existing systems and fiscal agent services with a modularized solution (i.e., Modularized Medicaid Enterprise System (MMES)) that will streamline the administration and oversight of its health care programs. The Medicaid Enterprise System (MES) requires expanding the current concept of a traditional MMIS (i.e., focused on claims payment) to become a system that not only processes claims but is also able to process clinical and administrative data to provide a comprehensive view of all members for all federal and state health care programs administered by the DOM enterprise. The underlying technology of the MES is being deployed in a cloud-based environment. Dustin's responsibilities include:

- Reviews all Cloud infrastructure system architecture and design documentation
- Reviews security/privacy documentation including system security plans produced by the vendor
- Reviews disaster recovery/business continuity documentation produced by the vendor
- Reviews and provides advice on project management documentation, federal and state security/privacy compliance

Project Reference			
Name	Aleeta Massey	**Telephone**	601-359-6050
Project Role	DOM Project Manager		

California Department of Social Services, Child Welfare Digital Services (CWDS)

CWDS-NS Transition Project Security Assessment

Information Security SME | September 2017 – March 2018 & March 2019 – Present

Jeff is the lead security analyst for independent verification and validation (IV&V) on the Checks and Balances Team. Jeff conducts independent security control assessments that include verifying appropriate risk management plans and standards are followed as well as interviewing & documenting discussions with project team, PMO, SI. The security assessments utilize NIST SP 800-53A R4 (including the Cyber Security Framework (CSF)) during the assessments of security and privacy controls, as well as FIPS (in Federal Information Systems and Organizations) and reference the California SAM requirements as guidance. During the independent security assessments, Jeff helps develop Security Project Plans involving status reports delivery, managing state resource requirements, working with stakeholders on report drafts, reviews, and submission. Also, Jeff manages to report on resource & project status, accomplishments, risks, issues, and other concerns (in the auditing and report delivery activities).

Jeff's information security responsibilities include reviewing the system security plan and the project's POA&M. Jeff is also conducting reviews of technical controls work (network, system & application) and makes Security recommendations in security documents, which are based upon NIST SP 800-53A R4, SP 800-66 (An Introductory Resource Guide for Implementing the HIPAA Security Rule), and best practices for information security for federal, state, and local agencies).

Project Reference			
Name	Will Friesen	TELEPHONE	(916) 225-2440
Project Role	Project Contract Manager		

California Department of Justice (DOJ), Network Information Security Unit

IT Security Policy Update Project

Information Security SME | June 2018 – June 2019

Jeff was the lead security analyst conducting analysis and research to revise DOJ IT Network Security policies, standards, and procedures. The goal of the project was to improve DOJ's compliance to security requirements and align policy with industry standards (including the NIST Cybersecurity Framework, International Standards Organization (ISO), California SAM, California Justice Information System standards, Open Web Application Security Standards, and other applicable policies and standards). Jeff reviewed the technical controls work (network, system & application), interviewed & documented discussions (with the project team, project PMO, and other stakeholders), and helped develop the Security Project Plan. Jeff ensured status reports delivery, state resource requirements and worked with stakeholders on report drafts, reviews & submission, and completed reporting on resource & project status, accomplishments, risks, issues, and other concerns. Also, Jeff performed a gap analysis, which helped ensure that security and privacy requirements were supported (i.e., traceable) to existing policies and standards. When completed, the project resulted in entirely new IT security policies, standards, and procedures that brought DOJ into alignment with industry standards.

PROJECT REFERENCE			
NAME	Todd Ibbotson	TELEPHONE	O: (916) 210-5045 C: (916) 838-9421
PROJECT ROLE	DOJ Information Security Officer		

Wells Fargo Bank

Disaster Recovery & Business Continuity Plan

V&V Information Security SME & IV&V Analyst | January 2000 – December 2006

Jeff was an information security analyst on the host-based Intrusion Detection Team; and assisted in the architecture, design, build, deployment, management, oversight, and monitoring of full host intrusion detection systems (HIDS), network intrusion detection systems (NIDS) , wireless intrusion detection systems (WIDS), business continuity planning (BCP) and disaster recovery (DR) implementations comprised of 144,000 end-users systemwide, which spanned more than six (6) years. Jeff was also responsible for helping to develop a Security Project Plan, which involved periodic status reports delivery, managing state resource requirements, working with stakeholders on report drafts, reviews, and submission.

Jeff is certified by Wallis and Futuna in BCP Design and Management. He has provided a formal IV&V assessment that included physical, logical, remote, and on-site testing to verify appropriate risk management plans and standards were being followed. The security assessments utilized Sarbanes-Oxley, National Institute of Standards and Technology, PCI-DSS (as well as other prioritized controls). During the IV&V functions, Jeff participated in managing the design, build, deployment, monitoring, auditing, and report delivery activities.

As a liaison member of the Computer Security Incident Response Team, Jeff was responsible for interviewing & documenting discussions with project team members, PMO, and the system integrator (as well as Privacy officers). Jeff participated in technical controls work (network, system & application) with other client System Analysts at the Data Center.

Jeff also participated in international investigations that related to system-wide, Information Security incidents; and was responsible for reporting on resource & project status, accomplishments, risks, issues, and other concerns.

PROJECT REFERENCE			
NAME	Greg Roll	**TELEPHONE**	(415) 595-8643
PROJECT ROLE	Wells Fargo Technology Manager		

EDUCATION

- Master of Science, Cyber Security, and Information Assurance | National University (NSA Center of Excellence) – La Jolla, CA
- Bachelor of Science, Criminal Justice Administration | California State University, East Bay – Hayward, CA

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- CompTIA CySA+
- National Security Agency NSTISSI 4011 National Training
- Standard for Information Security Systems Professional
- National Security NSTISSI 4012 National
- Information Assurance Training Standard for Senior Systems Managers
- TLO Advanced Course: Cyber Security-High Technology Threats
- Eclipse IV&V® Certification—Associate
- Windows Forensic Environment On-Scene Triage

- Certified Microsoft Technology Associate (MTA)
- POST: Critical Incident Response
- FEMA: ISO 100, 200, 400

Technical Skills

- **Hardware:** Servers, Workstations, Laptops, Tablets, Cell Phones, WIFI, Network Appliances, Switches, Routers, Arduino, Raspberry PI
- **Software:** Microsoft Office, Windows, Linux, Ubuntu, Kali
- **System Administration:** Microsoft Exchange, NT Domain Administration, send mail, POP3, Windows NT/2000 Server, Cisco Routers/Switches, Firewalls, VPN, DNS

Dustin Heath, Solutions Architect

Security & Privacy SME

Relevant Qualifications
Minimum of three (3) years of SCA experience: Dustin has approximately five years of experience performing the testing and evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended; and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Must show past SCA work on at least one (1) eligibility engagement that supported a state Medicaid system: Dustin has managed and coordinated SCA work on the TennCare ATP and TEDS (Deloitte NextGen) Eligibility systems in Tennessee. He's also involved in the Mississippi Department of Medicaid Modularized MES project.
Security and Privacy certifications: Dustin had been a Certified Information Systems Security Professional (CISSP), since 2005.
Experience developing security project plans: Dustin has managed the development, partner coordination, and review of System Security Plans based on MARS-E, SSA TSSR, and IRS SSR's (as well as NIST 800-53r4) with the states of Alabama, Tennessee, and Mississippi. This experience included status reports delivery, state resource requirements, and working with stakeholders on report drafts, reviews, and submission.
Deloitte NextGen experience: Dustin worked with Deloitte's security team over the past four years within the TennCare Enterprise Security and Privacy Teams from project inception through go-live in the summer of 2019.

Relevant Project Experience

Tennessee Division of TennCare

Medicaid Modernization Project

Project Manager & Security SME | January 2016 – Present

Tennessee is currently pursuing a Medicaid Modernization Project in which all aspects of the state Medicaid program are being updated to current technologies and capabilities per the ACA. Dustin provides program management services for the Division's IT security staff, vendors, and contractors.

This engagement involves oversight, reporting, and management of the requirements, design, and implementation of technical services following federal, state, and TennCare security and privacy requirements. Dustin's responsibilities include:

- Manages and participates in the creation, review, and submission of the MARS-E System Security Plan, SSA's Technical System Security Requirements (TSSR), and IRS Safeguards Security Report for the Deloitte NextGen Eligibility System (before the July 2019 Go-Live of the Eligibility system from project inception)
- Manages and coordinates the monthly POA&M tracking and reporting for CMS with the state Medicaid Agency, partner agencies, and vendors for the prior and current Eligibility system
- Manages and coordinates the Third-Party Security Controls Assessment, IRS, and SSA Onsite audit activities (for the Deloitte NextGen eligibility system in 2019) as well as weekly IRS Corrective Action Plans (CAP's) implementation for IRS reporting (pre and post-go-live
- Performs security program management services for TennCare Enterprise Security IT team that involves tracking of tasks for various projects within the security group. These responsibilities include:
    - Management of MARS-E 2.0 compliance based on NIST 800-53r4 security compliance

  - Security Team representative to vendor/partner security teams for the creation of System Security Plans required by the state agency for various Medicaid systems or modules (e.g., PBM, HIE, etc.).
  - Vendor coordination.
  - Service provider coordination;
- Trains and assists in the creation of System Security Plans and control documentation
- Identifies, owns, and manages risks/issues for various initiatives for the Enterprise Security Team, and provides recommendations for improvement

PROJECT REFERENCE			
NAME	Victor Patuzzi	**TELEPHONE**	(615) 507-6030
PROJECT ROLE	TennCare Chief Security Officer (CSO)		

Mississippi Department of Medicaid (DOM)

Modularized Medicaid Enterprise System

IV&V Security SME | February 2016 – Present

Dustin is the IV&V Security and Disaster Recovery SME for the client. The client's goal is to replace its existing systems and fiscal agent services with a modularized solution (i.e., Modularized Medicaid Enterprise System (MMES)) that will streamline the administration and oversight of its health care programs. The Medicaid Enterprise System (MES) requires expanding the current concept of a traditional MMIS (i.e., focused on claims payment) to become a system that not only processes claims but is also able to process clinical and administrative data to provide a comprehensive view of all members for all federal and state health care programs administered by the DOM enterprise. The underlying technology of the MES is being deployed in a cloud-based environment. Dustin's responsibilities include:

- Reviews all Cloud infrastructure system architecture and design documentation
- Reviews security/privacy documentation including system security plans produced by the vendor
- Reviews disaster recovery/business continuity documentation produced by the vendor
- Reviews and provides advice on project management documentation, federal and state security/privacy compliance
- Provides ongoing security advisory services for DOM

PROJECT REFERENCE			
NAME	Aleeta Massey	**TELEPHONE**	601-359-6050
PROJECT ROLE	DOM Project Manager		

Georgia Department of Banking and Finance (DBF)

Project Gold Software-as-a-Service (SaaS) Implementation

IV&V Specialist | July 2016 – July 2019

Dustin was the IV&V SME for DBF's initiative that replaced its legacy Paradox/Delphi system. The State felt that continued reliance on the existing systems was not sustainable since the system lacked functionality, interoperability, and scalability (needed by the DBF). The legacy system contained defects and security vulnerabilities that could no longer be supported by vendors. The new cloud-hosted system was DBF's system of record for regulated entities and related administrative and examination processes. The strategic objective was accomplished through Project GOLD, which had a target completion date of Fiscal Year 2019. Dustin's responsibilities included:

- Performed and reviewed all Cloud infrastructure and security/privacy documentation produced by the vendor

PROJECT REFERENCE			
NAME	Chris Roberts	TELEPHONE	770-986-1633
PROJECT ROLE	Department Project Manager		

Alabama Medicaid Agency

Integrated Eligibility System (CARES)

IV&V Consultant | June 2014 – February 2015

CARES was a multi-year, multi-agency project with the CMS, Alabama Medicaid Agency. The Alabama Department of Public Health Service sought to create a Cloud-based, statewide health and human services Eligibility determination and Enrollment Information System. Dustin performed the following services during this engagement:

- Reviewed infrastructure architecture and system security in a cloud-based environment
- Reviewed and recommended improvements to security artifacts for submission to the federal government (MARS-E 2.0 – IRS 1075, NIST 800-53r4)
- Developed monthly status reports
- Conducted analysis of crucial project methodologies to include risks, requirements, scheduling, testing, interfaces, data conversion, and implementation and turnover
- Developed and managed project issues and risk register
- Provided agency recommendation to improve project management processes and procedures

PROJECT REFERENCE			
NAME	T.J. Nola	TELEPHONE	(334) 353–4749
PROJECT ROLE	CARES Program Director		

Tennessee Department of Education

Multi-Vendor Student Information System and Data Warehouse

Staff Chief Technology Officer | June 2012 – July 2014

Dustin led the staff and leveraged external vendors in infrastructure operations initiatives to support over 130 public school districts, including Identity Management Systems (IMS) and Data Warehousing in a Windows Azure environment. Dustin's responsibilities included:

- Served an instrumental role in the Windows Azure-based implementation of the public/private dashboard system for distribution of education metrics to statewide educators
- Developed overall program strategies for multiple projects, while leading the business case and architecture strategy
- Spearheaded the first implementation of Azure-based Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) in the Tennessee state government
- Served as the hands-on lead creating specifications for technology implementations in new capital projects; examples of these projects include:
    - Redesign of campus-wide network connectivity (fiber, wired, and wireless)

  - Emergency notifications (for hearing-impaired students)
  - Digital voice and video
  - On-premise data room
  - Wireless design
  - Construction of a high school;
- As a member of the executive leadership team, he grew relationships with vendors, partners, and customers through personal interaction and communication
- Recruited and managed project managers, business analysts, and technical staff, both full-time equivalent and contract, for large-scale projects and ongoing operations

PROJECT REFERENCE			
NAME	Renee Koch	**TELEPHONE**	(615) 532–9027
PROJECT ROLE	Deputy Chief Information Officer, Department of Human Services		

Tennessee Department of Transportation

Staff Deputy Director (Deputy CIO), Information Technology | January 2012 – June 2012

The project sought services to provide oversight, direction, leadership, and coordination of efforts for all technology operations (including data center, help desk, geographic information systems (GIS), telecommunications, and enterprise application services). Dustin performed the following services:

- Used a hands-on approach, led implementations of statewide active directory migration, system center product line, application life cycle assessment, and ITIL assessment for the department's non-consolidated IT enterprise
- Set policy and procedures on project management methodologies, system development life cycles, and quality management for the IT enterprise
- Participated in the planning and budget of more than $33 million for the second-largest agency in the state, including multi-year information systems projections
- Directly responsible for more than 6,000 internal and external users for all aspects of technology operations

Tennessee Department of Transportation

Multiple Projects

Project Manager & Infrastructure Manager | July 2007 – January 2012

Dustin was accountable for planning and directing internal IT infrastructure projects and IT service management initiatives. Dustin's responsibilities included:

- Created project proposals and cost/benefit analysis for IT projects annually for inclusion in the information systems plan
- Managed highly visible, cross-functional projects to ensure programs were completed on time, within budget, satisfying scope requirements, and adhered to planned technical architecture
- Defined role requirements, managed consulting resources, and refined the methodology for executing program activities
- Led the creation of processes/master workflows for systems and application discovery and the definition of deliverables for multiple project threads relevant to the following models:
  - Datacenter migration
  - Disaster recovery
  - Business continuity

  - Service desk
- Standardized virtualization platform on Microsoft Hyper-V, dramatically reducing the cost to deploy new services cutting time-to-deploy by over 90% and helping to extend the usable life of an existing data center
- Performed current, gap, and target state analyses leading to conceptual and “living” technical documentation
- Developed network tools strategies for analysis, monitoring, and management of enterprise systems
- These activities paved the way for reliable critical systems, including construction management financial payments and public safety systems

PROJECT REFERENCE			
NAME	Renee Koch	TELEPHONE	(615) 532–9027
PROJECT ROLE	Deputy Chief Information Officer, Department of Human Services		

CORE Business Technology

Multiple Projects

Senior Consultant | January 2007 – June 2007

Dustin analyzed, designed, and documented the enterprise network and computer systems for the small and medium space. Dustin’s responsibilities included:

- Produced technology assessments, statements of work, and organized project assets to meet timeline objectives for small and medium-sized companies
- Deployed various Microsoft technologies for public and private sector clients
- Reviewed, developed, and presented deliverables for client management review and acceptance
- Provided gap analysis for systems in the areas of physical security, server, and application resiliency
- Participated in technical planning processes with managers and technical teams for project definition and delivery within the PCI compliance arena

PROJECT REFERENCE			
NAME	Joel Jenson	TELEPHONE	855-267-3287
PROJECT ROLE	Senior Consultant		

Insight Enterprises

Multiple Projects

Senior Consultant | Technical Architect | June 2004 – January 2007

Dustin served as the project/program director and technical architect and was responsible for large-scale contracts providing IT services. Dustin also:

- Provided client companies with solutions for complex technical and life cycle management requirements
- Developed favorable pricing structures with vendors while leveraging the company’s turnkey solutions and support to win several significant accounts
- Performed risk assessment projects to determine appropriate security, disaster recovery, and business continuity strategies

- Served as the project manager and technical lead for a global information security consulting services contract for a Fortune-100 company
- Served as the Project Manager/Technical Lead for information security and disaster recovery consulting services contract the largest US prepaid wireless carrier
- Performed a variety of regulatory compliance control assessments as well as penetration testing and vulnerability assessments for customers in the national security practice (HIPAA, PCI/DSS, COBIT, and SOX)
- Worked with numerous customers in a consulting capacity producing statements of work, current state assessments, and RFP/RFI responses related to resiliency engineering

PROJECT REFERENCE			
NAME	Rick Foote	TELEPHONE	813-637-7000
PROJECT ROLE	Senior Consultant		

EDUCATION

- Major: Computer Science | Wichita State University – Wichita, KS
- Major: Criminal Justice | Butler County Community College – El Dorado, KS

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Project Management Professional (PMP®) | Project Management Institute
- Certified Scrum Master (CSM) | Project Management Institute
- Certified Scrum Product Owner
- Microsoft Certified Systems Engineer (MCSE)
- Microsoft Certified Trainer Alumni
- HP/Compaq Accredited Systems Engineer