PUBLIC
CONSULTING
GROUP

State of West Virginia

Department of Administration

Workforce West Virginia Contingency Plan Validation

RFQ # WWV12103

Technical Proposal

August 18, 2011 1:30 PM

PUBLIC
CONSULTING
GROUP

August 18, 2011

Mr. Frank Whittaker
Department of Administration
Purchasing Division, Building 15
2019 Washington Street, East
Charleston, WV 25305-1030

Dear Mr. Whittaker:

With its mission to strengthen West Virginia's economy by supporting the economic stability and quality of its workforce, the Workforce West Virginia Unemployment Compensation (UI) Division is responsible for administering unemployment to the state's unemployed workers. To provide the best service to its citizens and to ensure the availability and resiliency of information systems critical to Workforce West Virginia's mission, the State seeks an independent verification and validation (IV&V) audit of the Unemployment Insurance (UI) Division's Contingency Plan.

With a history of over 24 years supporting state government across North America, Public Consulting Group, Inc (PCG) brings a wealth of experience and understanding of Unemployment Insurance and supporting information technology systems. PCG has carried out IT and UI program related projects in over 10 states including Arizona, California, Massachusetts, New York, North Carolina, Tennessee, Texas, Washington, and West Virginia.

PCG, with over 900 consultants across 33 offices in North America and Canada, is one of the nation's leading consulting firms in providing state agencies with fiscal, regulatory, programmatic, and operational advice and assistance, including information technology, feasibility studies, project management, independent validation and verification, project quality assurance, business continuity planning, and security assessments.

PCG understands the vendor is to conduct an independent verification and validation (IV&V) audit of the Unemployment Insurance (UI) Contingency Plan which has been developed by a separate vendor, and certify its compliance with the NIST Special Publication 800-34 standard.

We will conduct the Contingency Plan Audit services in accordance with the requirements set forth in your Request for Quote (RFQ) document.

We have experience in NIST audit projects of a similar scope and size and with conducting technology validation and verification assessments in general.

PCG brings a world class methodology based on the information technology standards from such organizations as the Institute of Electrical and Electronics Engineers (IEEE), International Organization for Standardization (ISO), NIST, and the Capability Maturity Model Integration (CMMI) of the Carnegie Mellon University Software Engineering

Institute (SEI). Three recent examples include a NIST based risk assessment for the State of California Employment Development Department, a NIST based risk assessment of the California Department of Industrial Relations, and a NIST based risk assessment of the North Carolina Employment Security Commission. PCG is currently providing Independent Verification and Validation (IV&V) services for the California Employment Development Department with two (2) multi-year projects including the replacement of the UI system and a build-out of its call center and Computer Telephony Integration system. Comprehensive Security Assessments are critical deliverables for each of these projects.

Our team has extensive experience assisting states in implementing large scale IT programs/projects through IV&V, Enterprise Technical Architecture Assessments and procurement support projects.

We bring a highly qualified team to carry out the services described in our proposal.

With our experience carrying out similar NIST audits we offer the State of West Virginia an extremely experienced team who will ensure all deliverables are achieved in accordance with the expectations and timeframes established by the Workforce West Virginia UI Division. Our lead principal auditor, Mr. Mike Bedford CISSP, CISA, CBCP, CISM has over 12 years of compliance and auditing experience, having worked on many significant government systems throughout the country. His expertise includes the identification, assessment and implementation of controls to assure resiliency of critical systems and orderly recovery processes. He has in depth experience and knowledge of business continuity best practices, NIST procedure guidance, and technologies that enable a resilient enterprise.

We thank you for the opportunity to submit this proposal to the Workforce West Virginia UI Division. Should questions arise or if you need additional information regarding the services offered, please do not hesitate to contact me at (916) 565-8090, or by email mbrazier@pcgus.com.

Sincerely,

Matt Brazier
Chief Operating Officer
Public Consulting Group Technology Consulting

Table of Contents

Table of Figures

Table of Tables

1. Cost Sheet

Table 1: Costs by Deliverable

Deliverables	Price
Evaluation of work products produced by the IT Contingency Plan vendor	$15,000
Present written documentation in electronic form of findings & recommendations confirming the Contingency Plan Vendor's work product included all seventeen key elements recommended by NIST SP800-34 as shown in Attachment I	$10,000
Presentation to WorkForce to describe findings & recommendations	$2,200
Final IV&V report including documentation of questions and answers presented during the presentation of findings & recommendations	$7000
TOTAL	$34,200

Note: Invoice for all services provided under this RFQ must be dated and received by WorkForce West Virginia by December 15, 2011.

Payment will be made upon completion of all deliverables as outlined in this RFQ.

2. Executive Summary

PCG will conduct an audit of the Unemployment Insurance (UI) contingency plan based on the following methodology. First the project team will assemble and review all relevant UI contingency plan documentation. Relevant documentation will include: the contingency plan itself, any related IT technical standards, test plans and results, business impact assessments, and other supporting documentation. Interviews will be scheduled with key stakeholders to confirm their participation in the creation of the contingency plan, to address any inconsistencies in the documentation and to obtain further supporting data. The initial data gathering and interview process will be conducted on site.

Next, the team will conduct a gap analysis measuring the UI contingency plan against the recommendations in the National Institute of Standards and Technology (NIST) 800-34 standard. Areas on non-compliance will be noted along with recommendations for bringing weak or missing controls into compliance. The PCG Lead Auditor will ensure that the seventeen key elements from NIST 800-34, which have been identified in the RFQ, are present in the plan, and will evaluate the effectiveness of the documented controls as designed by the vendor who created the contingency plan.

Once the initial gap analysis is complete, the PCG team will provide WorkForce West Virginia staff with recommendations in electronic (Microsoft Word) format describing how any identified deficiencies in the Contingency plan could be addressed.

Finally, the PCG team will schedule a presentation to describe its findings and recommendations to WorkForce West Virginia staff in person. At this presentation, PCG will respond to questions and provide clarifications regarding the presented recommendations. These questions and responses will be included in the final IV&V report in electronic (Microsoft Word) format. The Lead Auditor will sign the report, indicating that a qualified auditor and business continuity professional has completed an independent evaluation of the plan and stands by the findings.

The duration of engagement will be approximately 8 weeks, including a two-week gap to allow the WorkForce Team to review and comment on the recommendations prior to the presentation. The PCG Team will consist of a Lead Independent Verification and Validation (IV&V) Auditor and a Project Manager, both with significant experience in assessing NIST based security and contingency plans. Figure 1 depicts the proposed audit approach.

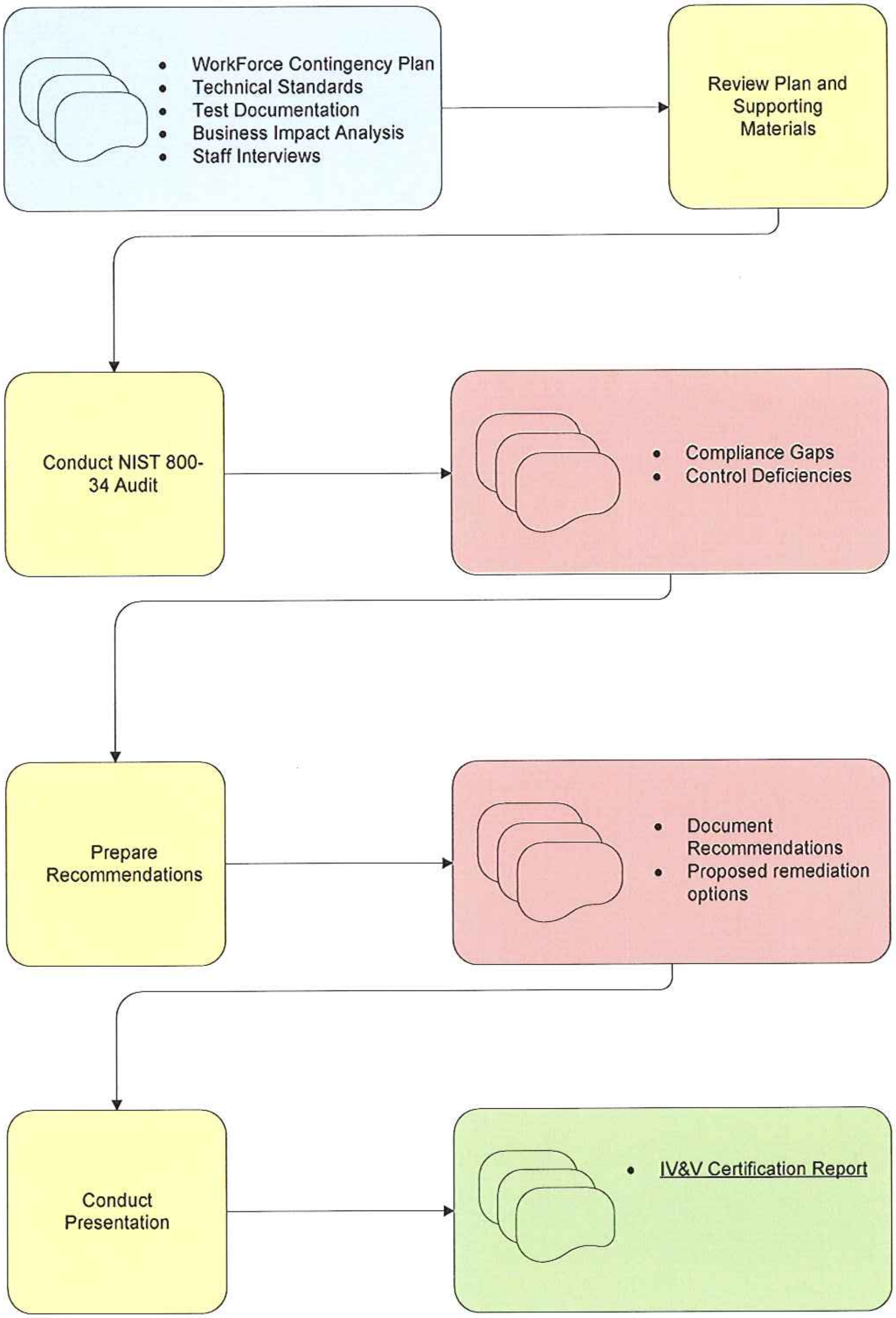

Figure 1: Contingency Plan Audit Process

3. Detailed Response

3.1. Assessment of the Work to be Performed and Timeline

The WorkForce West Virginia Unemployment Insurance Division has requested an independent verification and validation (IV&V) audit of their recently completed UI Contingency Plan. An independent vendor developed the plan on behalf of WorkForce to address operational contingencies for the UI Division's IT services. The desired outcome of the IV&V audit is a formal written report certifying the plan's conformity with NIST 800-34 Rev. 1, Contingency Planning Guide for Information Technology Systems, published in May, 2010. The IV&V audit work is to be completed between September 1, 2011 and November 30, 2011. PCG has read and assessed the requirements, deliverables, and timelines from the RFQ and determined the stated parameters to be feasible and appropriate. A key requirement to facilitate successful project completion within the stated time frame will be pre-staging of the WorkForce documentation for streamlined access and review.

3.2. Approach

PCG will conduct a kickoff meeting to identify stakeholders, to gain an understanding of the overall UI IT environment, and to review the tasks and deliverables with the WorkForce team. The first major task will be to assemble and review all relevant UI contingency plan documentation. Relevant documentation will include: the contingency plan itself, any related IT technical standards, test plans and results, business impact assessments, and other supporting documentation. Based on the team's evaluation, interviews will be scheduled with key stakeholders to address any inconsistencies in the documentation and to obtain further supporting data. The initial data gathering and interview process will be conducted on site.

Next, the team will conduct a gap analysis measuring the UI contingency plan against the recommendations in the NIST 800-34 standard. Areas of non-compliance will be noted along with recommendations for bringing weak or missing controls into compliance. The PCG Lead Auditor will ensure that all required NIST 800-34 elements are present in the plan, focusing on the seventeen key elements of NIST 800-34 highlighted in the RFQ, and will evaluate the effectiveness of the documented controls as designed. These key NIST 800-34 areas are to be assessed:

- Purpose
- Applicability
- Scope
- Record of Changes

- System Description
- Line of Succession
- Responsibilities
- Activation Criteria
- Documented Notification Procedures
- Damage Assessment Procedures
- Detailed Recovery Procedures
- Reconstitution Phase Procedures
- Contact Information of CP teams
- Vendor contact Information
- Checklists for system recovery
- Equipment/System requirements lists
- Description/Direction to Alternative sites.

The initial gap analysis will identify all the plan elements expected to be present in a plan based on NIST 800-34 and the RFQ, a list of all elements present in the UI Contingency Plan, a list of all missing elements, and an assessment of the effectiveness of the included plan elements.

Once the initial gap analysis is complete, the PCG team will develop a detailed document confirming that all seventeen key elements are included in the work product of the Contingency Plan Vendor. This document will also detail the IV&V audits findings and recommendations, describing how any identified deficiencies in the IT Contingency plan could be addressed by Workforce. Upon delivering the findings, WorkForce will have an opportunity to review the findings prior to the presentation.

A Final Certification Report, detailing the compliance status of the UI Contingency Plan, will be developed based on the IV&V audit findings. Any residual deficiencies will be documented with a reference to the related recommendations. The Lead Auditor will sign the report, indicating that a qualified auditor and business continuity professional has completed an independent evaluation of the plan and stands by the findings.

Table 2 below details the proposed high-level tasks and schedule associated with the PCG approach to conducting the UI Contingency Plan IV&V audit work. PCG has developed the schedule to ensure completion within the allotted time frame in the event of a late start or other unforeseen project delays.

Table 2: Tasks and Schedule

Task Name	Duration	Start	Finish
Kickoff Meeting	1d	Tue 9/6/11	Tue 9/6/11
Data Gathering	5d	Wed 9/7/11	Tue 9/13/11
Staff Interviews	5d	Wed 9/7/11	Tue 9/13/11
Plan Analysis	5d	Wed 9/14/11	Tue 9/20/11
Develop Initial Gap Analysis	5d	Wed 9/21/11	Tue 9/27/11
Develop Recommendations	3d	Wed 9/28/11	Fri 9/30/11
WorkForce Feedback	15d	Mon 10/3/11	Fri 10/14/11
Management Presentation	1d	Mon 10/17/11	Mon 10/17/11
Develop Final Report	8d	Tue 10/18/11	Thu 10/27/11
Closeout	1d	Fri 10/28/11	Fri 10/28/11

3.3. Technical Capability

We have experience in Independent Validation and Verification projects of a similar scope and size and with conducting security assessments in general.

Our team has extensive experience assisting states in conducting large scale IT development and implementation, independent verification and validation, enterprise architecture assessments and procurement projects. PCG has extensive experience with Federal Standards compliance, and brings a world class methodology based on the information technology standards from such organizations as the Institute of Electrical and Electronics Engineers (IEEE), International Organization for Standardization (ISO), and the Capability Maturity Model Integration (CMMI) of the Carnegie Mellon University Software Engineering Institute (SEI). Two recent examples include a Technical Architecture Alternatives Analysis (TAAA) for the State of California Department of Social Services (CDSS), $133 million Child Welfare Services/Case Management System (CWS/CMS), and RFP development and procurement support for the State of California Department of Social Services (CDSS) $244 million Case Management and Information Payrolling Project (CMIPS) Replacement Project. We have also completed a security assessment of the Los Angeles Unified School District's medical billing interface with the State's Medicaid reimbursement system. Current ongoing projects include:

- Providing Independent Verification and Validation services for the California Employment Development Department in a multi-year project to replace its UI system and build out its call center and Computer Telephony Integration system. Security Assessments are critical deliverables for each of these projects.

- Managing a corrective action plan for the State of Washington Department of Labor and Industries information security program addressing remediation requirements to bring L&I into compliance with NIST 800-53 Rev. 3 and IRS Publication 1075 security standards.

3.4. RFQ Requirements

Requirement 1. The Contractor will conduct a detailed IV&V audit and provide a detailed recommendations document based upon the requirements in the Statement of Work, in a timeline consistent with the needs of WorkForce as spelled out in the RFQ.

PCG Response: In Section 3.2, PCG has provided a detailed description of its approach to conducting the UI Contingency Plan IV&V audit work. The approach section includes a task list and proposed timeline for completing the project as specified and within the requested time window.

Requirement 2. Provide three references of prior work of a similar nature.

PCG Response: Section 5 of this document provides three PCG client references.

Requirement 3. Identify personnel and provide resumes for those who will work on this project.

PCG Response: Section 4 of this document provides resumes for the proposed PCG team and provides a detailed description of their qualifications to perform the work requested by WorkForce West Virginia.

Requirement 4. Project costs must be effective and efficient.

PCG Response: PCG has provided a cost proposal that provides WorkForce with an outstanding value relative to the capabilities of our team and the quality of our deliverables.

Requirement 5. Available start date and completion date must fall within the targeted period of performance of September 1, 2011 to November 30, 2011.

PCG Response: The PCG team is available to start on or about September 1st 2011 and based on our proposed schedule, will complete the work well before the November 30th deadline.

Requirement 6. Vendors must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia.

PCG Response: PCG is currently licensed in the State of West Virginia and is in good standing with any and all state and local laws and requirements by any state or local agency of West Virginia.

4. Staffing

PCG proposes a highly qualified and experienced team consisting of a Lead IV&V Auditor and a Project Manager. Together, the team members bring over 30 years of IT experience, significant business continuity and disaster recovery planning experience, and unmatched expertise in conducting IV&V assessments for UI programs.

4.1. Project Role: Lead IV&V Auditor

Michael Bedford, CISSP, CBCP, GCSC, CISA, CISM

Director of Enterprise Security / Information Security Officer
PCG Technology Consulting

Summary

Michael Bedford is the Director of Enterprise Security and PCG Information Security Officer. Mr. Bedford has over 13 years of enterprise technology security experience and is a highly accomplished system design architect. Mr. Bedford has significant experience in many public and private sectors, including criminal justice, government, healthcare, banking, public utilities and e-commerce. His areas of expertise include enterprise risk management, security policy development, risk assessment, security training, regulatory guidance and compliance (HIPAA, FISMA, SOX, GLB, PCI, IRS), business continuity and disaster recovery, data confidentiality and protection, access control and authentication, network security design, and incident response and forensic analysis. Mr. Bedford has expert level knowledge of many diverse technologies including, Unemployment Insurance systems, Medicaid Management Information Systems, Tax accounting and collection systems, Eligibility determination systems, Criminal Justice Information systems. He also possesses in depth knowledge and hands on experience of many security control systems, including encryption and key management, preventative and detective control measures (IDS, Antivirus, SPAM filtering, patch management solutions, vulnerability scanners, etc.). Mr. Bedford is an expert in industry security control standards including NIST 800 series, ISO 27000 series, COBiT, FIPS and more. Mr. Bedford is a proven project leader and technical architect with strengths in both project and resource management. His keen business acumen coupled with expert leadership skills and industry knowledge enables Mr. Bedford to provide tangible results that continually exceed client expectations.

Experience

PCG Technology Consulting **9/2005—Present**

California Employment Development Department (EDD) **5/2006—Present**

Unemployment Insurance Modernization IV&V

Title on Project: Senior IV&V Consultant, Security Subject Matter Expert

Project Description: EDD is undertaking a complete overhaul of their customer service and call center operations and application to include the latest technology like Enterprise architecture and SOA approaches to IT service delivery. As Independent Validation and Verification (IV&V) PCG is responsible for ensuring the Project adheres to IEEE and ISO standards in the procurement, design, and delivery of the solution.

Michael Bedford, CISSP, CBCP, GCSC, CISA, CISM

Director of Enterprise Security / Information Security Officer
PCG Technology Consulting

Responsibilities: As lead security subject matter expert, responsibilities include verifying appropriate risk management plans and standards are being followed, RFP security review; solution architecture security assessment; product vulnerability and risk assessment; and disaster recovery/ business continuity plan validation and verification

California Employment Development Department (EDD) **1/2007—Present**

Automated Collections Enhancement System IV&V

Title on Project: Senior IV&V Consultant, Security Subject Matter Expert / Technical Architect

Project Description: EDD is building a new Automated Collections Enhancement System to increase collection of owed tax revenue within the State. The Project is a benefits based procurement for a new software collection system. PCG Technology Consulting serves as the Independent Validation and Verification on the project, ensuring the client, the vendor, and the solution effectively manages risks and reflects industry best practices.

Responsibilities: Responsibilities include providing requirements traceability, security control validation and recommendations, risk assessment of proposed designs, implementation plans, and rollout strategies. As lead security subject matter expert and lead architecture subject matter expert, responsibilities also include verification of data confidentiality, coding vulnerability identification, and solution assessment against EDD security policies and standards and IRS Publication 1075 requirements.

Rhode Island Department of Health Services **8/2010—Present**

Global Waiver an Medicaid MITA IT Planning

Title on Project: Lead MMIS System Architect

Project Description: Rhode Island requires IT strategic planning and RFP development for key Medicaid initiatives to position the State to address Healthcare Reform, Health Insurance Exchange, Health Information Exchange, federal MITA requirements, and Eligibility determination. PCG is to develop a strategic IT roadmap, IT systems architecture, and applicable RFPs to meet these business drivers.

Responsibilities: Responsibilities include providing business requirements traceability to IT solutions mapping, assessment of current capability and process maturity (MITA), General Systems Design (GSD) Plans for the 'to-be' state encompassing the current and future needs of the Department, technology roadmap to implement the GSD, alternatives analyses with associated costing estimates, development and submission of a Implementation APD for federal cost sharing, and development of a MMIS replacement RFP and an Eligibility system RFP.

Michael Bedford, CISSP, CBCP, GCSC, CISA, CISM

Director of Enterprise Security / Information Security Officer
PCG Technology Consulting

Duties include: technical project management, systems architecture and systems design, leading multiple joint design sessions, interfacing with the State IT organization, business and technical requirements definition, system capabilities assessment, etc.

California Department of Health Services **5/2010—Present**

CA-Medicaid Management Information System IV+V

Title on Project: Technology Subject Matter Expert / Security Subject Matter Expert

Project Description: California has awarded a contract for the takeover of the existing State MMIS system to a new vendor. PCG provide Independent Validation and Verification services to ensure the project's success. IVV services will include system design review, transition plan review and assessment, organizational change management assessment, and technology (application, infrastructure, network) analysis

Responsibilities: Responsibilities include providing technical analysis of proposed technologies, plans, security controls, testing plans, and project management activities.

Duties include: leading security evaluation of the System Security Plans, MITA assessment, subject matter expertise and consultation with State and vendor proposed designs and integration/cutover plans.

California Department of Justice (DOJ) **9/2005—7/2010**

California Law Enforcement Telecommunication System

Title on Project: Senior Security Consultant, Project Lead

Project Description: Assess California Law Enforcement Telecommunication System (CLETS) for adherence to state law, security best practices, FBI Criminal Justice Data requirements (CJIS) and system hardening and recommend control enhancements. CLETS is a large collaboration network that ties in all California and federal criminal justice entities for real time criminal data involved in criminal activity investigation, patrol stops (wireless access in patrol cars), arson review (fire investigation).

Responsibilities: Review of all CLETS policies and procedures for compliance with state and federal law, FBI mandated Criminal Justice Information Systems requirements, FIPS standards, and internal DOJ constraints. Duties included reviewing/assessing/auditing all connected agencies for compliance with defined practices, policies and procedures including technical system design review, and formulating recommendations for compliance. Duties were expanded to include security advisor to the DOJ on all high profile security related matters and proposals and security policies and standards development including liaison to the FBI for policy decisions regarding national criminal justice security standards.

Michael Bedford, CISSP, CBCP, GCSC, CISA, CISM

Director of Enterprise Security / Information Security Officer
PCG Technology Consulting

North Carolina Department of Labor and Industrial Relations **7/2009—12/2009**

Employment Security Commission security assessment

Title on Project: Senior Auditor

Project Description: NCESC is mandated by federal requirements as a recipient of Federal Parent Locator Data to undergo an external triennial security assessment of its IT systems and IT operations for adherence with security standards and best practices (NIST 800-53)

Responsibilities: Lead and conducted an independent audit of the NCESC network against the NIST 800-53 control recommendation standard using the NIST 800-30 Risk Assessment methodology. Provided NCESC and federal government with an approved security audit and Plan of Action and milestones to remedy noted deficiencies. Conducted a thorough security risk assessment of the State central IT data center and operations, and the ESC department IT operations supporting confidential data.

California Housing Finance Agency **2/2007—10/2008**

Business Continuity Plan (BCP) Development

Title on Project: Senior Consultant; Business Continuity Planner

Project Description: The California Housing Finance Agency required a comprehensive Business Continuity Plan (BCP) as part of its enterprise risk management program. The project charter was to develop a BCP from the ground up using best practice techniques including conducting a Business Impact Assessment, Risk Assessment, and development of a Disaster Recovery Plan for IT systems.

Responsibilities: Responsibilities included leading the development of an Incident Management Plan, individual Business Resumption Plans, Communication Plans, and the Operational Recovery Plan (IT business resumption) as major components of the BCP. The project also included mock disaster and table top exercises and training for senior staff and emergency management teams.

Duties included: managing the project, the clients' expectations and the overall education of the senior staff on common business continuity concepts using the DRII and SEMS/NEMS standards. Lead a team that mapped out the entire Agency and its critical services, dependencies, and developed recovery time objectives (RTO) for these services. Developed a technical Operational Recovery Plan to meet the RTOs using sophisticated virtualization technology. Provided a comprehensive mock disaster drill and training for the Emergency Management Team.

Michael Bedford, CISSP, CBCP, GCSC, CISA, CISM

Director of Enterprise Security / Information Security Officer
PCG Technology Consulting

Los Angeles Unified School District **6/2008—9/2008**

LAUSD Security Risk Assessment (Medical Billing)

Title on Project: Senior Auditor

Project Description: LAUSD was required by the State to conduct an independent security risk assessment of its paperless Medical Billing System for claims submitted electronically to the State Medicaid system. This assessment included a technical vulnerability evaluation of the system, an assessment of the IT administrative support controls, and physical security of the data center.

Responsibilities: Lead and conducted an independent audit of the LAUSD network against the NIST 800-53 control recommendation standard using the NIST 800-30 Risk Assessment methodology. Provided LAUSD with risks to the system ranked based on impact and likelihood of exploitation. Presented detailed control recommendations and action plan to mitigate the critical risks identified in the audit to executive management.

California Department of Health Services **2/2006—7/2006**

CA-Medicaid Management Information System Assessment

Title on Project: Senior Consultant / MMIS Security Subject Matter Expert

Project Description: The California Department of Health Services (CDHS) Payment Systems Division (PSD) requested the assistance of PCG to perform a technical assessment of the California Medicaid Management Information System (CA-MMIS) and to propose options for continued claims processing for the State of California. CDHS Management needs to determine the most cost-effective manner to plan how the aging CA-MMIS will meet on-going challenges of system modification for improving the services it provides.

Responsibilities: The security assessment provided two major deliverables. The first deliverable was to provide insight for CDHS as to the maturity and effectiveness of the CA-MMIS security plan and related controls. The goal was to validate that the security plan and associated controls were adequate to meet regulatory (HIPAA) and business demands. The second deliverable was to provide an assessment of the Eligibility Interface to the FAME system. This involved assessing the security of the external web transaction presence and data protection while eligibility inquiries and updates are being processed by CA-MMIS (confidentiality, integrity, and authorization). The assessment also included specific recommendations based on best security practices to remedy noted deficiencies.

Michael Bedford, CISSP, CBCP, GCSC, CISA, CISM

Director of Enterprise Security / Information Security Officer
PCG Technology Consulting

Federal Home Loan Bank, San Francisco **6/2004—9/2005**

Manager/Technical Lead, Enterprise Architecture and Security

Professionally lead the core architecture, operations and security team in the 24x7x365 transaction intensive, $160 billion banking business, while achieving record availability, customer satisfaction, and operating cost reduction. Designed, secured, and planned a multiple region network that consisted of Development, Test/QA and Production networks across multiple data centers and disaster recovery sites.

- Conducted SOX review and remediation plan that included the overhaul of Problem, Change, Configuration management procedures
- Lead incident response teams in analyzing, repairing, and reporting of security incidents
- Created security policies and procedures to meet both public and private regulatory compliance requirements
- Was instrumental in the development and implementation of ITIL aligned security processes and procedures
- Performed risk assessments/vulnerability assessment of key business critical systems (including financial reporting, project tracking, and transaction based financial operations)
- Prepared for, and passed multiple independent internal and external security audits and risk assessments
- Developed and deployed many core infrastructure services, including DNS, DHCP, Exchange 2000/2003, SQL 2000, IIS 5 and 6, GPOs, File/Print services, etc.
- Developed and deployed a business continuity plan that made expert use of advanced virtualization, clustering, and SAN technologies
- Developed and delivered professionally lead training for senior management and peers alike on subjects such as access control, encryption, engineering principles and design, and policy and procedure creation

DirectApps **12/2003—6/2004**

Manager/Technical Lead, Enterprise Architecture and Security

Project Director/Lead for multiple projects with Health and Human Services Agency Data Center that included (but not limited to):

- Remote access solutions and VPN (IPSEC, Citrix Secure Access Manager)
- Secure application serving for sensitive health related applications
- Designed a new collaboration network for the California Health Officers Association of California (HOAC) that allowed instant, highly secure collaboration in the event of catastrophic bio-terrorism attacks
- Created security policies and procedures to meet both public and private regulatory compliance requirements
- Created and lead technical instruction for subordinate staff in the areas of system design, enterprise security, and encryption techniques and methodologies
- Was entrusted with the role of Enterprise security advisor and was chartered with the creation and subsequent implementation of enterprise security policies

Michael Bedford, CISSP, CBCP, GCSC, CISA, CISM

Director of Enterprise Security / Information Security Officer
PCG Technology Consulting

McKesson Corporation **1/2001—12/2003**

Senior Consultant/Team Lead

Provided progressive technical leadership and sustainable results for Fortune 20 Company by engineering, deploying, and supporting business automation, architecture, and new technologies. Lead and directed all aspects of multi-million dollar projects for mission-critical, high availability systems, including project teams, architectural designs, security reviews and assessments, engineering, network security, implementation, and maintenance oversight. Oversaw activities as Lead Consultant of global teams consisting of administrators, engineers, architects, and security experts from project inception through completion of enterprise services design and deployment.

- Created policies and procedures for enterprise-class services' administration management, security issues, disaster recovery plans, and change management
- Designed and implemented enterprise security policies and procedures to ensure industry and regulatory compliance (HIPAA/Sarbanes Oxley)
- Lead teams in the design, documentation, and assessment of ePHI containing systems and related technologies (encryption, backup and recovery, access control standards, etc.)
- Technical team lead and direct interface between customers and IT solutions engineering, managing a multitude of parallel project design and engineering
- Designed a global Exchange 2003/ADS 2003 that leveraged EMC SAN technologies to facilitate enterprise collaboration initiatives, while reducing costs by consolidating over 30 directory structures into one single fault tolerant infrastructure
- Developed and delivered professionally lead training to senior management and subordinates in the areas of system architecture, security concepts, policies and procedures, and risk mitigation practices

iMotors, Inc. **3/2000—1/2001**

Senior Consultant/Manager of Technology

Responsible for all aspects of managing a national IT infrastructure from policy and procedure creation, to overseeing multi-million dollar project implementations of state of the art of call centers in a 24x7 environment. Provided strategic consulting in the creation of an IT governance model for meeting e-commerce security and industry requirements. Provided expert leadership in the creation of business IT processes for meeting the IT governance model using the Microsoft Operations Framework (MOF) and security controls as prescribed through CoBIT and COSO for application and infrastructure security.

- Achieved optimal network uptime and reliability by initiating procedures to measure performance, providing 3-tier troubleshooting and analysis, and proactively resolving problems via open communication lines
- Performed all top-level system administration and design functions
- Chief system design architect for e-commerce based application development and supporting infrastructure
- Establishing system build standards and automation
- Security design implementation and security audit compliance liaison

Michael Bedford, CISSP, CBCP, GCSC, CISA, CISM

Director of Enterprise Security / Information Security Officer
PCG Technology Consulting

TekSystems/AreoTEK **1998—3/2000**

Senior Consultant/Project Lead

Provided technical expertise and consultative services for a diverse clientele on contract basis. Ensured all clients' networking and system design needs were identified and met, increasing efficiency, reducing costs, and enhancing usability. Common contracts were for high profile customer projects that required specific technology expertise and leadership skills.

- Served as Y2K Network Engineer for Catholic Health Care West upgrading software/ hardware on a multitude of networks and servers throughout Northern California
- Senior level network design architect / engineer for mid tier enterprise businesses
- Incident response technical lead for containing, repairing, and preventing security related issues (malicious code, virus/worms, hack attempts, audits, etc.)
- Responsible for interfacing senior management for solution and ROI presentation models

Education

BS, Computer Engineering, California State University, Sacramento

AS, Computer Engineering, Yuba Community College, Marysville

Certifications

- Certified Information Systems Security Professional (CISSP) – 10 yrs
- SANS GIAC Certified Security Consultant (GCSC) – 6 yrs
- Certified Information Systems Auditor (CISA) – 5 yrs
- Certified Information Security Manager (CISM) – 4 yrs
- Certified Security Professional (CompTIA Security+) – 8 yrs
- HIPAA Certified Professional (CHP) - 7 yrs
- HIPAA Certified Security Specialist (CHSS) – 7 yrs
- Certified Technical Trainer (CompTIA CTT+) – 8 yrs
- Microsoft Certified Trainer (MCT) – 7 yrs
- VMWare Certified Professional (VCP) – 8 yrs
- Microsoft Certified Systems Engineer Windows 2003 (MCSE Windows 2003) – 8yrs
- Microsoft Certified Systems Engineer Windows 2000 (MCSE Windows 2000) – 11 yrs
- Microsoft Certified Systems Engineer NT 4.0 (MCSE NT 4.0) – 13 yrs
- Microsoft Certified Systems Administrator for Windows 2003 (MCSA Windows 2003) -8 yrs
- Microsoft Certified Systems Administrator for Windows 2000 (MCSA Windows 2000)- 11 yrs
- Microsoft Certified Professional + Internet (MCP+I) – 13 yrs
- Citrix Certified Administrator XP 1.0 (CCA) – 11 yrs
- ITIL Certified (ITILF) – 7 yrs
- Certified Business Continuity Professional (CBCP) - 5 yrs

Michael Bedford, CISSP, CBCP, GCSC, CISA, CISM

Director of Enterprise Security / Information Security Officer
PCG Technology Consulting

Professional Affiliations

Information Systems Security Association (ISSA)

Information Systems Audit and Control Association (ISACA)

American College of Forensic Examiners (ACFEI)

Special Skillsets

Program Knowledge: HIPAA Compliance, ISO 27000 series; BS 17799; NIST/FIPS standards (NIST 800-53, NIST 800-30, FIPS 197, FIPS 142, etc.); SOX; GLB; SB 1386; Criminal Justice Information Security (CJIS) Policies; Information Technology Infrastructure Library (ITIL); Microsoft Operations Framework (MOF); Business Continuity Planning, Disaster Recovery Planning, Enterprise Architecture, Security Planning & Assessments, Technical Architecture Assessments, Policy and Procedure Analysis, Regulatory Compliance Assessment and Remediation, Incident Response planning, Software/System Development Life Cycle; Directory Services and Single Sign on (SSO), ITIL Assessment and remediation; Technology Solutions Development and Implementation, etc.

Hardware: IBM eSeries x86 Servers, HP Proliant x86 Servers; Dell PowerEdge x86 Servers; Cisco PIX/ 65xx/ Catalyst/ASA series networking devices and appliances; ESS/EMC/HP/McData/Cisco SAN hardware; IBM Z Series mainframes IBM I/P series UNIX systems; Multiple NAS systems; wide range of tape backup systems and libraries; full range of PDUs; assortment of authentication devices (biometrics/proximity/Key FOB/etc), etc.

Network: Routers, Firewalls, Intrusion Detection/Prevention Systems, Network Protocols (TCP/IP, IPX, etc.), DNS, DHCP, WINS, Cisco, Nortel, WiFi, SAN fabric networks, PBX/Cisco VoIP and UNITY; VPN solutions (SSL, VPN client, etc.)

Platforms: Windows NT 4.0 Server (all versions), Windows 2000 Server (all versions), Windows Workstation (all versions), Windows Server 2003 (all versions), Windows 2007 (all version) RedHat Advanced Server, VMWare ESX / GSX, Cisco 65xx/PIX/VoIP/VPN, SAN technologies, (ESS/EMC/HP/McData/Cisco) HPUX, IBM P Series, Sun Solaris x86, CICS, etc.

Software: All MS Office products, .NET and BackOffice Servers (Exchange, SMS, SQL, IIS, Terminal Server, Application Center, IAS, etc.) Remedy, VMWare, Citrix, Siebel, SAP, Netware, Terminal emulators, QIP, PeopleSoft, assortment of network and system management software (HP OpenView, Tivoli, MOM, etc.), Oracle, FileMaker Pro; Directory Services, J2EE, Forensic tools; vulnerability and network scanners (MBSA; Foundstone; Nessus; Snort; CoreImpact), ACF, RACF, etc.

Databases: Microsoft SQL 2000/2005, Oracle 8i/9i/10g; MySQL; DB2, ADABAS, etc.

4.2. Project Role: Project Manager

Andrew Riley, CISSP / CEH

Director, PCG Technology Consulting

Summary

Andrew Riley is a Director with PCG Technology Consulting. Mr. Riley is an IT Architect and information security expert with over 18 years of diverse IT experience. Areas of expertise include: Datacenter Design, Systems Architecture, Planning and Assessment, Regulatory Compliance, Project Management, Training, QA/IV&V, Business Analysis and Testing.

Relevant Project Experience

State of Rhode Island DHS **10/2010—Present**

Medicaid Global Waiver/MITA IT Planning

Title on Project:	Technical Expert
Project Description:	The State of Rhode Island Department of Health Services has contracted with Public Consulting Group to conduct a MITA Self Assessment and develop procurement RFP's and required Implementation Advanced Planning (IAPD) documentation.
Responsibilities:	In the role of Medicaid IT Technical Expert, responsible for assessing and analyzing existing IT assets (people, processes, and technology) and those required to support the Global Waiver program. Andrew has conducted interviews of key IT stakeholders from the State and their current Medicaid fiscal agent. Andrew is responsible for assessing current Medicaid data across the enterprise and comparing against HIE (Health Information Exchange) and HCA (Health Choice Account) requirements. This process will result in the creation of a gap analysis and "to-be" General System Design (GSD).

State of Washington DIS **3/2010—9/2010**

State Data Center Project

Title on Project:	Chief Datacenter Architect
Project Description:	The State of Washington Department of Information Services is building a new $100 million state data center with the intent of migrating all existing services and consolidating smaller agency data centers into the new facility. DIS needed an architect to lead the design process for core infrastructure and private cloud services in the new state data center SDC and to support move planning for existing services. Core infrastructure included: network, security, storage and high-density compute environments.
Responsibilities:	In the role of Chief Data Center Architect, led a team of 14 DIS and agency engineers to develop architectural documents, functional narratives, detailed design diagrams, and technical decision papers for datacenter and cloud computing solutions. Performed feature analysis of major OEM vendors, identified gaps in existing services, and developed detailed functional and technical requirements. Worked closely with the CISO, Director of Operations, Executive Steering Committee, and State Enterprise

Architects representing, server, storage, and network disciplines. Developed draft technical standards for virtualization security controls related to multi-tenancy and cloud computing. Redesigned security controls resulting in improved serviceability, enhanced capabilities, and estimated capital cost savings of over $2 million.

State of Washington DSHS **4/2008—3/2009**

Provider Compensation Project

Title on Project: QA/IV&V Manager

Project Description: DSHS needed to develop an RFP for the replacement of a mainframe-based provider payment system for individual providers. Based on a feasibility study, an application service provider (ASP) model was selected. The new solution was required to interface with the Provider One MMIS system via Washington's Enterprise Service Bus. The size and complexity of the project required the use of outside QA/IV&V support to assess the project approach and effectiveness.

Responsibilities: In the role of QA/IV&V Manager, assessed technical project approach, system designs, and deliverables for compliance with standards and best practices. Provided assessments of budgets, schedules, and project scope. Recommended process improvements related to requirements management. Assessed project risk/issues management process to ensure timely mitigation. Assessed progress toward identified business and technical objectives. Assessed vendor performance and oversight activities. Continuously monitored the project environment, to include project organizational structure, project plans and changing conditions that might affect the project success. Assessed staff capabilities, utilization, and management. Identified and reported on project risk. Assessed stakeholder involvement and recommend improvements to project communications.

State of Washington DSHS **5/2006—4/2008**

Washington MMIS Replacement Project

Title on Project: Senior IV&V Analyst

Project Description: The Provider One project replaced the legacy mainframe MMIS system with a new J2EE based e-CAMS Medicaid platform and RuleIT rules engine. The new MMIS solution was a combination of COTS products in a SOA architecture and included cloud-based SaaS services. DSHS contracted for an IV&V team to focus on technical approach, deliverables and testing.

Responsibilities: In the role of Senior IV&V Analyst, performed technical assessments of SOA-based architecture, interfaces, software testing, deployment, security and operations management for the State of Washington Medicaid Management Information System (MMIS) replacement project. Performed on-site interviews and assessments of DD&I vendor processes and procedures. Validated unit, system, integration, and UAT testing results. Reviewed methodologies and made recommendations in the areas of security, data conversion, testing, operations, interfaces and change management. Developed draft role based access control (RBAC) standards and access evaluation criteria. Developed data handling standards for ePHI.

State of Oregon DHS **6/2006—11/2008**

Oregon SACWIS (ORKIDS)

Title on Project: Planning and QC Technical Lead

Project Description: The State of Oregon Department of Human Services contracted for Planning and Quality Control support for the implementation of a Statewide Automated Child Welfare System (SACWIS). The project encompassed initial planning, technical requirements elicitation and documentation, RFP development, and deliverable quality reporting.

Responsibilities: In the role of QC Systems and Security Lead, reviewed vendor processes and deliverables for the Oregon Statewide Automated Child Welfare Information System (SACWIS) replacement project. Led a team of state staff and contractors to develop as-is technical documentation for the legacy system. Developed technical requirements, DDI RFP, and IAPD documentation. Developed deliverable quality metrics based on ISO, NIST, and IEEE standards. Reviewed and assessed DDI vendor deliverables and made recommendations for technical improvements.

State of Oregon DHS **6/2005—4/2008**

Oregon MMIS Replacement Project

Title on Project: Security Expert – QA / IV&V

Project Description: The State of Oregon Department of Human Services replaced its legacy MMIS system with a new web-based solution based on a transfer system from the state of Oklahoma. DHS contracted for an IV&V team to focus on technical approach, deliverables and testing.

Responsibilities: In the role of Systems and Security Lead, reviewed vendor processes and deliverables for the Oregon MMIS replacement project. Performed risk analysis and tracked compliance with State Information Security policy, HIPAA, ISO 17799, NIST and OWASP standards. Placed particular emphasis on layered defenses and secure coding techniques. Performed security code review of .NET and C Unix code modules. Developed test plans to ensure secure implementation. Provided regular reporting to project management and the executive steering committee. Developed deliverable quality metrics based on ISO, NIST, and IEEE standards. Reviewed and assessed DDI vendor deliverables and made recommendations for technical improvements.

Andrew Riley, CISSP / CEH

Director, PCG Technology Consulting

California Cancer Registry / Public Health Institute **1/2004—8/2004**

HIPAA Security Policy Development

Title on Project: Senior Security Consultant

Project Description: The California Cancer Registry (CCR) is a public-private partnership between the State of California and the Public Health Institute for the purpose of providing cancer research. CCR was in the process of consolidating its regional registry databases into a single state-wide system at the time that the HIPAA Security regulations went into effect. CCR contracted for security consulting services to bring them into compliance with the HIPAA Security Rule and develop key security policy works.

Responsibilities: Developed HIPAA compliant information security policies for a major California public health organization. Updated requirements documents based on HIPAA draft security requirements to reflect final rules and relevant California statutes such as SB1386. Designed security policies for streamlined compliance audit. Conducted a business impact analysis and developed business continuity strategies and unit-level contingency plans. Led a policy gap analysis for the 8 CCR regional registries to identify issues and mitigation strategies.

Employment History

PCG Technology Consulting	**9/2010—Present**
22nd Century Consulting -Contract	**3/2010—9/2010**
Network Computing Architects	**10/2009—3/2010**
Comsys –Contract	**8/2009—10/2009**
Systest Labs-Contract	**5/2006—3/2009**
IPSpecialties, LLC	**11/2002—5/2006**
Holocom Systems	**11/2001—5/2002**
Verado	**6/1998—11/2001**
THIS Computer Solution	**1/1998—6/1998**
Portland General Electric	**6/1996—1/1998**
Hewlett Packard –Contract	**7/1995—6/1996**
US ARMY	**4/1991—4/1995**

Education

BS Business -IT Management, Western Governors University (In progress)

US Army Field Artillery School, Diploma -Digital Systems

Andrew Riley, CISSP / CEH

Director, PCG Technology Consulting

Training/ Certifications

CISSP #32487, Certified Ethical Hacker (C|EH) #ECC932427, ITIL v3 Foundation Certified, MCSE #390019, McAfee Technical Professional (Risk and Compliance Management and Data Protection), Gartner Certified Associate -IT Project Management.

Inactive Certifications: Certified Information Privacy Professional (CIPP/G), Microsoft Certified Trainer (MCT), Checkpoint Certified Security Administrator, Sonicwall Certified Security Administrator, Radware Intelligent Application Switching Engineer, Novell CNA (Intranetware and GroupWise)

Professional Development

- Program Chair, Information Systems Security Association –Portland Chapter 2009
- ITIL v3 Foundation Course 2009
- SANS Institute -Security Essentials Track, 2001
- Checkpoint Software Technologies Ltd. -Firewall 1/VPN1 (NG) Management I and II, 2001
- Gartner Institute -IT Project Management Track, 2000

Special Skillsets

Experience: Datacenter architecture and design, Cloud Security architecture, virtualization, Cisco UCS and HP C7000 blade architectures, storage virtualization technologies, hypervisor-level firewalls and IDS, Information Security and Privacy program development, compliance strategy, IT Audit, security assessment and testing, Sarbanes-Oxley, HIPAA/HITECH, FACTA/Red Flags, GLBA/FFIEC, COBIT, NIST 800, ISO 27001, PCI-DSS, ITIL, NERC/CIP, business continuity planning, classroom security training, awareness training, incident response, secure network design concepts, firewall technologies – Palo Alto Networks, Checkpoint, Sonicwall, Fortinet, BlueCoat Proxy SG, ArcSight, RSA Data Loss Prevention, enVision, McAfee DLP, Foundstone Enterprise, McAfee IPS/NAC, Dragon IDS, enterprise antivirus suites, LANguard, Nessus, Nmap, Maltego, Nikto, Cenzic Hailstorm, Protocol Analyzers, OS Hardening, VMware, Microsoft Windows Servers 2003/2008, Database security , Red Hat/Fedora, VPN using IPSEC, PGP, RFP and requirements development, requirements management.

5. References

5.1. State of California, Employment Development Department

Unemployment Insurance Modernization Project

May 2006 to Present

Scope of Work:

PCG provided IV&V services as Prime Contractor to EDD. This IV&V project included the following activities:

- **Security Assessment**. Provide a Physical and Informational Assets Security assessment. Conduct NIST SP 800-18, and NIST SP800-30 Risk Assessments using NIST SP 800-53. Review and validate NIST SP 800-37 Security Certification.
- **Task Management.** Development and maintenance of Task Accomplishment Plan, Software Verification & Validation Plan in accordance with IEEE 1012-2004 standards, and Project Work plan in adherence to PMBOK guidelines.
- **System Development and Architectural Oversight.** Critical assessments of vital system functionality, identifying internal and external impacts. Provide analysis or evaluation in the following areas:
  - Software Development Lifecycle risk analysis
  - Development hardware configurations
  - Proposed System architecture
  - Configuration Management
  - Interfaces
  - System Security Plan
- **Testing Oversight.** Review, witness and evaluate the following test plans, procedures, requirements, environment, tools and execution during each phase:
  - Integration Test
  - System Test
  - User Acceptance Test
  - Security Testing

Implementation, Transition and Operations Oversight. Monitor and evaluate system change request management during Design, Development and Implementation (DDI). Evaluate system defect tracking, knowledge transfer activities, and operational recovery plans and processes.

Project Team: The following PCG employees worked on this project:

- Michael Bedford, PCG Director of Enterprise Security
- Andrew Riley, PCG Director of Pacific Northwest Services

Reference: Please contact the following individuals for information on PCG's work:

Mark Smith, Manager of Project Oversight
Information Technology Branch, MIC 71
800 Capitol Ave.
Sacramento, CA 95814
(916) 654-8252
Mark.Smith@edd.ca.gov (916) 654-8252
Mark.Smith@edd.ca.gov

5.2. State of North Carolina, Employment Security Ccommission

Security Risk Assessment

July 2009 to December 2009

Scope of Work:

With its mission to promote and sustain the economic well being of North Carolinians in the world marketplace by providing high quality and accessible workforce-related services the Employment Security Commission (ESC) of North Carolina provides employment services, unemployment insurance, and labor market information to the State's workers, employers, and the public. One of ESC's responsibilities is the National Directory of New Hires (NDNH) which connects with the Office of Child Support Enforcement (OCSE). As part of this program OCSE expects each state agency that receives NDNH information to have an independent company evaluate the security controls that ensure that Federal Parent Locator Service (FPLS) information received from the OCSE is protected.

To assist ESC in meeting its obligations, PCG was asked to perform an independent security risk assessment of the Commission's internal systems and IT business practices. Tasks included:

- Perform an independent Security Risk Assessment of the IT Data Center and support functions
- Perform an independent risk Security Risk Assessment of the Commission's Central Office

- Developing, modifying and writing DOJ policies and procedures recommendations
- Creating, reviewing, editing, and presenting reports relative to ongoing system security events, issues, and requirements
- Writing issue papers
- Attending meetings, making presentations and conducting demonstrations
- Assisting NISU and DOJ staff in other technical support issues
- Any security related duties as necessary

Deliverables

The deliverables for this study included but were not limited to: documented security requirements, policies, procedures and recommendations; issue papers and reports; presentations; and recommendations to approve or deny CLETS applications.

Project Team: The following PCG employees worked on this project:

- Mike Bedford

Reference: Please contact the following individuals for information on PCG's work:

Joe Dominic, IT Security Specialist

California Department of Justice

4949 Broadway, Sacramento, CA 95820

(916) 227-1353

Joe.dominic@doj.ca.gov