

Attachment 10 includes a separate form (Excel file) for each Key Staff position and contains two (2) parts that must be completed for each proposed candidate:

Part 1 - Resume Tab

Instructions: Include a Resume for all proposed Key Staff. The template prescribes the required content that must be submitted with Proposals in response to the RFP. This format should also be used by the successful Contractor for the duration of the Agreement.

Key Staff Background: Provide Contractor name, Key Staff name, Role of Key Staff within the Contractor organization, duration (in years) in that Role and a description of the Key Staff's role within the organization.

Key Skills: Provide a summary of all skills and qualifications the proposed Key Staff candidate possesses in support of the Key Staff position.

Education/Certifications: Provide education and any relevant certifications. Start with the most recent.

Relevant Experience: This section is optional. For any Projects not cited within Part 2, contractors may provide additional Projects that illustrate experience or background to support their Key Staff candidate. Start with the most recent experience and add as many rows as necessary.

Part 2 - Key Staff Minimum Qualification Tabs (S31 - S36)

Instructions: Complete the Staff Project qualifications portion on each of the tabs of the form (all fields with a white background). All fields on the form must be completed, providing sufficient information to allow the Consortium to validate that the proposed Staff person meets the Minimum Qualifications (MQs).

For each Project, identify the name of the Project, Project/Project Role details, Description of the relevant Project Experience, and Project Contact information.

Project/Project Role details: Provide the Contractor name, Project start and end dates, percentage of time on the Project (100%, 50%, etc.), and name of Role on the Project.

Description of Relevant Experience: Provide a description that includes sufficient detail to verify that the Key Staff role/experience on the Project is relevant the MQ definition.

Contact Information: Provide the name, company/org name, role, email and phone number of a Client/Customer contact for this Project. Contact Information must be provided for a Project to be considered valid.

A full-time equivalent (FTE) is estimated to be approximately 1,920 hours annually. Proposed Staff may not cite full-time experience gained working simultaneously on multiple Projects.

If more than six (6) Projects must be cited in order to satisfy the MQ, insert the additional Project and Contact Information and a corresponding new summary table row.

Do not enter any data into the summary section of the tab. All summary table data will be populated from the Project details provided.

If a Project's start and/or end date is prior to the start time of the MQ or a Project does not comply with a specified Project detail, the form provides some basic "error" messaging. This messaging is informational. Contractors are responsible for the accuracy of their submissions and alignment of each Project with the details of the Minimum Qualifications (MQs).

BENEFITS CAL SECURITY MANAGER			
PART 1 – RESUME			
Contractor	Accenture		Candidate Name Ben Trogia
Position in the Company	Technology Delivery Lead Associate Director Project management, client relationship management, team leadership		Length of Time in Position 15 years
Project Position & Responsibilities	Security Manager Project responsibilities will be as defined in RFP section 11.1.3.6.9.		
Skills & Qualifications for Project Position	<p>Skills: Ben delivers security services and validates compliance with industry standards and privacy and security agreements (PSAs). He defines and implements security policies, strategies, procedures, and configurations to confirm confidentiality, integrity, and availability of his clients' environments and data. Ben serves as the focal point for cybersecurity solutions for Salesforce, AWS security platforms, and identity and access management (IAM). Ben delivers field-tested cyberthreat intelligence, security assessment, and threat modeling solutions while providing insight using security tools, including Akamai Web Application Security (WAF/DDOS), LogRhythm, Splunk, and Linux OS hardening. He possesses strong communication and collaboration skills across key stakeholders to define and implement a framework of solution security architecture to protect the environment. Ben responds promptly to security breaches and provides root cause analysis/mitigation plan to remedy the situation.</p> <p>Qualifications: Ben manages security solutions for large, complex public services applications. He is an SME for security and regulator standards, including CIS, MARS-E 1.0/2.0, NIST 800-53, HIPAA, California Statewide Information Management Manual (Simm), and California State Administrative Manual (SAM). Ben has 9.5 years of experience as a Security Manager directly responsible for collaborating with Application Development teams, technical architects, and security policy experts to define and implement an integrated framework of solution security architecture (MQ S31: Exceeds). For 9.5 of the past 11 years, he has served as a lead developing, implementing, improving, and monitoring industry standard security strategies, solutions, and processes on projects involving AWS cloud environments (MQ S32: Exceeds). Ben has 9.5 years of experience applying information security principles, methods, and techniques in the development of project security deliverables on projects involving large and complex IT systems (MQ S33: Exceeds). He has 9.5 years of experience assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) to identify appropriate security controls to protect personally identifiable information (PII), protected health information (PHI), and/or federal tax information (FTI) data (MQ S34: Exceeds). Ben has seven years of experience with systems that comply with the National Institute of Standards and Technology (NIST) 800-53 moderate baseline (MQ S35: Exceeds). He additionally holds an (ISC)2 Certified Information Systems Security Professional (CISSP) certification and will maintain it for the duration of the contract (MQ S36: Meets).</p>		
Education (add rows as needed)			
Start	End	Degree / Course of Study	School
8/1/2004	6/1/2007	B.S., Computer Information Systems	University of the Pacific
Professional Certifications or Designations (add rows as needed)			
Certification or Designation	Organization	Dates	
Certified Information Systems Security Professional (CISSP)	International Information System Security Certification	April 4, 2014 – April 30, 2025, Credential: 461611	
Project Management Professional (PMP)	Project Management Institute	March 2018 – March 22, 2027, Credential: 2179891	

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE					
Contractor -	Accenture		Candidate Name - Ben Trogia		
Minimum Qualification - S31	A minimum of three (3) years of experience as a Security Lead directly responsible for collaborating with application development teams, technical architects, and security policy experts to define and/or implement an integrated framework of solution security architecture.				
Project Name	Start Date	End Date	Percentage of Time	Duration in Months	Project Value
CalSAWS	4/1/2022	7/30/2024	34%	28.0	9.5
myCAvax	4/1/2022	7/30/2024	33%	28.0	9.2
CalCONNECT	4/1/2022	7/30/2024	33%	28.0	9.2
myCAvax	12/1/2020	3/31/2022	50%	16.0	8.0
CalCONNECT	12/1/2020	3/31/2022	50%	16.0	8.0
CalCONNECT	6/1/2020	11/30/2020	100%	6.0	6.0
California Healthcare Eligibility, Enrollment	3/1/2014	5/31/2020	100%	75.0	75.0
Totals				196.9	124.9

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS PROJECT DETAILS					
Minimum Qualification - S31		A minimum of three (3) years of experience as a Security Lead directly responsible for collaborating with application development teams, technical architects, and security policy experts to define and/or implement an integrated framework of solution security architecture.			
Project #1				Contact	
Company Name:		CalSAWS Consortium		Contact Name & Role:	Michele Peterson, Test/Release Manager Section Director
Project Name:		CalSAWS		Company/Org Name:	CalSAWS Consortium
Start Date (MM/DD/YYYY):		4/1/2022	End Date (MM/DD/YYYY):	7/30/2024	Phone Number:
Staff Role:		Security Manager	Percentage of Time:	34%	Email:
		As the Security Manager, Ben's accomplishments and responsibilities collaborating with Application Development teams, technical architects, and security policy experts to define and/or implement an integrated framework of solution security architecture include: Solution development <ul style="list-style-type: none">Oversees a Security team of 42 professionals (14 onshore, 28 offshore)Collaborates with Application Development teams, technical architects, the CalSAWS Security Operations Lead, and the CalSAWS Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the CalSAWS environment and dataAfter we enabled AWS Inspector, reviewed the security findings for the Lambda functions, then coordinated and organized the findings with the Application Development teamsArchitected, designed, and built different security solutions for Open Plan of Action and Milestones (POAMS)Collaborated with the CalSAWS privacy officer, CalSAWS ISO, and CalSAWS Security team to present the POAMS solutionsLed team that performed the architecture analysis and solution development to move CalSAWS' security posture from NIST 800-53 Rev 4 to Rev 5Collaborated with the CalSAWS privacy officer, CalSAWS ISO, and CalSAWS Security team to detail the NIST 800-53 Rev 5 solutionAssisted Linux and Windows team architects on implementing the CIS security standards to harden workstations that required detailed			

Description of relevant experience:	knowledge of the scripts			
	Reporting <ul style="list-style-type: none"> Maintains IS strategy (forward-looking roadmap), aligning services to the strategy Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk Responds promptly to security events/incidents and provides timely notification of incidents to the CalSAWS Security Operations Lead and the CalSAWS Privacy Officer of incidents, in accordance with requirements for security incident notification 			
	Compliance <ul style="list-style-type: none"> Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training following project onboarding/roll-on Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> Federal Information Processing Standard Publication 199 California Statewide Information Management Manual (SIMM) B40- California State Administrative Manual (SAM) HIPAA regulatory standards NIST 800-53: Security and Privacy Controls for Information Systems Organizations 			
Project #2				
Company Name:			California Department of Public Health	
Project Name:			myCAVax	
Start Date:			4/1/2022	End Date (MM/DD/YYYY): 7/30/2024
Staff Role:			Security Manager	Percentage of Time: 33%
			Phone Number:	
			Email:	
<p>As the Security Manager, Ben's accomplishments and responsibilities collaborating with Application Development and security policy experts to define and/or implement an integrated framework of solution security architecture include:</p> <p>Solution development</p> <ul style="list-style-type: none"> Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the Vaccine Management Program environment and data Led the design, development, and implementation of a DevSecOps solution for the Vaccine Management solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments Identifies information security weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on Developed and implemented the Vaccine Management Program's plans and procedures for business continuity and security incident management 				

Description of relevant experience:		<ul style="list-style-type: none"> Created, manages, and updates the Vaccine Management Program's System Security Plan that contains the project's security controls and procedures Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from vaccine hunters, Twitter bots, and malicious threat actors to protect vaccines when supply was limited 																																	
		Reporting <ul style="list-style-type: none"> Maintains IS strategy (forward-looking roadmap), aligning services to the strategy Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk Responds promptly to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification 																																	
		Compliance <ul style="list-style-type: none"> Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training following project onboarding/roll-on Created, updates, and manages the Vaccine Management Program's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the CalCONNECT solution Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> Federal Information Processing Standard Publication 199 California Statewide Information Management Manual (SIMM) California State Administrative Manual (SAM) HIPAA regulatory standards NIST 800-53: Security and Privacy Controls for Information Systems Organizations 																																	
<table border="1"> <thead> <tr> <th colspan="4">Project #3</th> <th colspan="2">Contact</th> </tr> </thead> <tbody> <tr> <td colspan="2">Company Name:</td> <td colspan="2">California Department of Public Health</td> <td colspan="2">Contact Name & Role:</td> </tr> <tr> <td colspan="2">Project Name:</td> <td colspan="2">CalCONNECT</td> <td colspan="2">Company/Org Name:</td> </tr> <tr> <td colspan="2">Start Date (MM/DD/YYYY):</td> <td>4/1/2022</td> <td>End Date:</td> <td>7/30/2024</td> <td>Phone Number:</td> </tr> <tr> <td colspan="2">Staff Role:</td> <td>Security Manager</td> <td>Percentage of Time:</td> <td>33%</td> <td>Email:</td> </tr> </tbody> </table>						Project #3				Contact		Company Name:		California Department of Public Health		Contact Name & Role:		Project Name:		CalCONNECT		Company/Org Name:		Start Date (MM/DD/YYYY):		4/1/2022	End Date:	7/30/2024	Phone Number:	Staff Role:		Security Manager	Percentage of Time:	33%	Email:
Project #3				Contact																															
Company Name:		California Department of Public Health		Contact Name & Role:																															
Project Name:		CalCONNECT		Company/Org Name:																															
Start Date (MM/DD/YYYY):		4/1/2022	End Date:	7/30/2024	Phone Number:																														
Staff Role:		Security Manager	Percentage of Time:	33%	Email:																														

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities collaborating with Application Development teams, technical architects, and security policy experts to define and/or implement an integrated framework of solution security architecture include:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the CalCONNECT environment and data • Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management • Created, manages, and updates the CalCONNECT project's System Security Plan (SSP) that contains the project's security controls and procedures • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors <p>Reporting</p> <ul style="list-style-type: none"> • Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds timely to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training after project onboarding/roll-on • Created, updates, and manages the CalCONNECT project's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the myCAvax solution • Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations
<p>Project #4</p>	<p>Contact</p>

Company Name:	California Department of Public Health			Contact Name & Role:	Ian Sanford, Security Architect
Project Name:	myCAVax			Company/Org Name:	California Department of Public
Start Date (MM/DD/YYYY):	12/1/2020	End Date (MM/DD/YYYY):	3/31/2022	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	50%	Email:	
	<p>As the Security Manager, Ben's accomplishments and responsibilities collaborating with Application Development and security policy experts to define and/or implement an integrated framework of solution security architecture included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the Vaccine Management Program environment and data • Led the design, development, and implementation of a DevSecOps solution for the Vaccine Management solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Identifies information security weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the Vaccine Management Program's plans and procedures for business continuity and security incident management 				

Description of relevant experience:	<ul style="list-style-type: none"> Created, manages, and updates the Vaccine Management Program's System Security Plan that contains the project's security controls and procedures Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from vaccine hunters, Twitter bots, and malicious threat actors to protect vaccines when supply was limited 				
	Reporting <ul style="list-style-type: none"> Maintains IS strategy (forward-looking roadmap), aligning services to the strategy Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk Responds promptly to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification 				
	Compliance <ul style="list-style-type: none"> Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training following project onboarding/roll-on Created, updates, and manages the Vaccine Management Program's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the CalCONNECT solution Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> Federal Information Processing Standard Publication 199 California Statewide Information Management Manual (SIMM) California State Administrative Manual (SAM) HIPAA regulatory standards NIST 800-53: Security and Privacy Controls for Information Systems Organizations 				
Project #5				Contact	
Company Name:	California Department of Public Health			Contact Name & Role:	Ian Sanford, Security Architect
Project Name:	CalCONNECT			Company/Org Name:	California Department of Public Health
Start Date (MM/DD/YYYY):	12/1/2020	End Date:	3/31/2022	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	50%	Email:	

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities collaborating with Application Development teams, technical architects, and security policy experts to define and/or implement an integrated framework of solution security architecture included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the CalCONNECT environment and data • Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management • Created, manages, and updates the CalCONNECT project's System Security Plan (SSP) that contains the project's security controls and procedures • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors <p>Reporting</p> <ul style="list-style-type: none"> • Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds timely to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training after project onboarding/roll-on • Created, updates, and manages the CalCONNECT project's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the myCAvax solution • Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations
<p>Project #6</p>	<p>Contact</p>

Company Name:	California Department of Public Health		Contact Name & Role:	Ian Sanford, Security Architect
Project Name:	CalCONNECT		Company/Org Name:	California Department of Public Health
Start Date (MM/DD/YYYY):	6/1/2020	End Date:	11/30/2020	Phone Number:
Staff Role:	Security Manager	Percentage of Time:	100%	Email:
	<p>As the Security Manager, Ben's accomplishments and responsibilities collaborating with Application Development and security policy experts to define and/or implement an integrated framework of solution security architecture included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the CalCONNECT environment and data • Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management • Created, manages, and updates the CalCONNECT project's System Security Plan (SSP) that contains the project's security controls and procedures • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the 			

Description of relevant experience:	<p>Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection</p> <ul style="list-style-type: none"> Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors 			
	<p>Reporting</p> <ul style="list-style-type: none"> Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk Responds timely to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification <p>Compliance</p> <ul style="list-style-type: none"> Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training after project onboarding/roll-on Created, updates, and manages the CalCONNECT project's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the myCAvax solution Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> Federal Information Processing Standard Publication 199 California Statewide Information Management Manual (SIMM) California State Administrative Manual (SAM) HIPAA regulatory standards NIST 800-53: Security and Privacy Controls for Information Systems Organizations 			
Project #7			Contact	
Company Name:	California Office of Systems Integration, Covered California		Contact Name & Role:	Thea Man; Deputy Chief Information Security Officer
Project Name:	California Healthcare Eligibility, Enrollment, and Retention System (CalHEERS)		Company/Org Name:	California Office of Systems Integration, Covered California
Start Date (MM/DD/YYYY):	3/1/2014	End Date:	5/31/2020	Phone Number:
Staff Role:	Security Manager	Percentage of Time:	100%	Email:

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities collaborating with Application Development teams, technical architects, and security policy experts to define and/or implement an integrated framework of solution security architecture included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Collaborated with Application Development teams, technical architects, the Covered California Chief Information Security Officer (CISO), and the Covered California Security Architect on the CalHEERS project to define and implement an integrated framework of security solution architecture • Built a comprehensive security program that aligned to standards from the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) 800-37 Risk Management Framework and 800-53 System Security Plan controls, and IRS Safeguard Procedures • Conducted information security risk assessments and privacy impact assessments annually • Validated security controls and processes using annual security control reviews in accordance with the Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E) standards, and reviewed results of reviews and recommendations with Covered California's CISO and Security Architect • Managed and tracked security gaps identified during assessments and audits using the CalHEERS project's Plan of Action and Milestones (POA&M) process • Developed and deployed complex identity and access management (IAM) solutions using the Oracle Identity and Access Management (IAM) platform for self-service registration, user provisioning, application authentication, and single sign-on with enterprise credentials • Enabled the provisioning and secure management of more than 20,000 internal users, 10 million Californians, and 100,000 concurrent users and met availability requirements of 98% <p>Reporting</p> <ul style="list-style-type: none"> • Led a Security team that managed security devices and responded to security events/incidents, including timely notification of incidents to the CISO and Security Architect in accordance with the CalHEERS project's requirements for security incident notification • Conducted routine weekly scanning of servers using the project's Qualys solution to identify and rank vulnerabilities delivered in summary and detailed reports so CalHEERS project leadership could prioritize remediation actions according to vulnerability threat and potential impact levels • Designed and conducted vulnerability and penetration testing to identify and test methods for exploiting vulnerabilities to circumvent or defeat the security features of the system and supporting infrastructure and provide recommendations for remediation and mitigation to the Covered California CISO and Security Architect • Supported the CalHEERS infrastructure, including assembling, configuring, and running various tests, such as manual and automated attack methods and tests for penetration testing <p>Compliance</p> <ul style="list-style-type: none"> • Adhered to security compliance and privacy requirement standards, including the Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E); Patient Protection and Affordable Care Act (PPACA); IRS Publication 1075 Tax Information Security Guidelines for federal, State, and local agencies; and State of California privacy requirements • Reviewed and maintained security measures, recommended actions, and implemented enhancements • Created, updated, and managed the CalHEERS project's System Security Plan, technical design documents and operational manuals for security tools, security architecture diagrams, and incident management procedures • Managed the application security testing program, which included scans of application code using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborated with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Created, updated, and managed the CalHEERS project's plans and procedures for disaster recovery and business continuity, and led the execution of restores for the CalHEERS data centers
---	--

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE					
Contractor -	Accenture		Candidate Name - Ben Trogia		
Minimum Qualification - S32	A minimum of three (3) years of lead experience within the past ten (10) years developing, implementing, improving and monitoring industry standard Security strategies, solutions, and processes on Projects involving an AWS cloud environment.				
Project Name	Start Date	End Date	Percentage of Time	Duration in Months	Project Value
CalSAWS	4/1/2022	7/30/2024	34%	28.0	9.5
myCAvax	4/1/2022	7/30/2024	33%	28.0	9.2
CalCONNECT	4/1/2022	7/30/2024	33%	28.0	9.2
myCAvax	12/1/2020	3/31/2022	50%	16.0	8.0
CalCONNECT	12/1/2020	3/31/2022	50%	16.0	8.0
CalCONNECT	6/1/2020	11/30/2020	100%	6.0	6.0
California Healthcare Eligibility, En	3/1/2014	5/31/2020	100%	75.0	75.0
Totals				196.9	124.9

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS PROJECT DETAILS					
Minimum Qualification - S32		A minimum of three (3) years of lead experience within the past ten (10) years developing, implementing, improving and monitoring industry standard Security strategies, solutions, and processes on Projects involving an AWS cloud environment.			
Project #1				Contact	
Company Name:		CalSAWS Consortium		Contact Name & Role:	Michele Peterson, Test/Release Manager Section Director
Project Name:		CalSAWS		Company/Org Name:	CalSAWS Consortium
Start Date (MM/DD/YYYY):		4/1/2022	End Date (MM/DD/YYYY):	7/30/2024	Phone Number:
Staff Role:		Security Manager	Percentage of Time:	34%	Email:
		As the Security Manager, Ben's accomplishments and responsibilities developing, implementing, improving, and monitoring strategies, solutions, and processes on projects involving an AWS cloud environment include:			
		<p>Solution development</p> <ul style="list-style-type: none">Oversees a Security team of 42 professionals (14 onshore, 28 offshore)Collaborates with Application Development teams, technical architects, the CalSAWS Security Operations Lead, and the CalSAWS Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the CalSAWS environment and dataDesigned, built, implemented, and operated a Qualys Endpoint Defection and Response (EDR) solution on all Windows and Linux servers, CalSAWS workstations, and County-managed workstations—12,000 devicesDelivered CalSAWS greater value by switching licenses while heightening the security posture through the EDR solutionDesigned, built, implemented, and operated a file integrity monitoring solution for CalSAWS Linux and Windows serversAfter we enabled AWS Inspector, reviewed the security findings for the Lambda functions, then coordinated and organized the findings with the Application Development teamsArchitected, designed, and built different security solution for Open Plan of Action and Milestones (POAMS)Collaborated with the CalSAWS privacy officer, CalSAWS ISO, and CalSAWS Security team to present the POAMS solutionsLed team that performed the architecture analysis and solution development to move CalSAWS' security posture from NIST 800-53 Rev 4 to Rev 5Collaborated with the CalSAWS privacy officer, CalSAWS ISO, and CalSAWS Security team to detail the NIST 800-53 Rev 5 solutionAssisted Linux and Windows team architects on implementing the CIS security standards to harden workstations that required detailed knowledge of the scripts			

Description of relevant experience:	Reporting <ul style="list-style-type: none">• Maintains IS strategy (forward-looking roadmap), aligning services to the strategy• Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk• Responds promptly to security events/incidents and provides timely notification of incidents to the CalSAWS Security Operations Lead and the CalSAWS Privacy Officer of Incidents, in accordance with requirements for security incident notification Compliance <ul style="list-style-type: none">• Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan• Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training following project onboarding/roll-on• Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data :<ul style="list-style-type: none">- Federal Information Processing Standard Publication 199- California Statewide Information Management Manual (SIMM)- California State Administrative Manual (SAM)- HIPAA regulatory standards- NIST 800-53: Security and Privacy Controls for Information Systems Organizations				
Project #2				Contact	
Company Name:	California Department of Public Health			Contact Name & Role:	Ian Sanford, Security Architect
Project Name:	myCAvax			Company/Org Name:	California Department of Public Health
Start Date:	4/1/2022	End Date (MM/DD/YYYY):	7/30/2024	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	33%	Email:	
	<p>As the Security Manager, Ben's accomplishments and responsibilities developing, implementing, improving, and monitoring strategies, solutions, and processes on projects involving an AWS cloud environment include:</p> <p>Solution development</p> <ul style="list-style-type: none">• Develops, implements, improves, and monitors industry-standard security strategies, solutions, and processes on the Vaccine Management Program's large, complex IT systems, including Salesforce and AWS cloud environments• Responsible for development and deployment of cybersecurity solutions, protection of personal information, digital information, and security compliance• Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture• Led the design, development, and implementation of a DevSecOps solution for the Vaccine Management solution's Salesforce application that includes scanning of application code in AWS environments via dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST)• Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments• Identifies information security weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards• Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on• Developed and implemented the Vaccine Management Program's plans and procedures for business continuity and security incident management• Created, manages, and updates the Vaccine Management Program's System Security Plan that contains the project's security controls and procedures• Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution				

Description of relevant experience:	for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection <ul style="list-style-type: none"> Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from vaccine hunters, Twitter bots, and malicious threat actors to protect vaccines when supply was limited 			
	Reporting <ul style="list-style-type: none"> Maintains IS strategy (forward-looking roadmap), aligning services to the strategy Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk Responds timely to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification Compliance <ul style="list-style-type: none"> Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training after project onboarding/roll-on Created, updates, and manages the Vaccine Management Program's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the CalCONNECT solution Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> Federal Information Processing Standard Publication 199 California Statewide Information Management Manual (SIMM) California State Administrative Manual (SAM) HIPAA regulatory standards NIST 800-53: Security and Privacy Controls for Information Systems Organizations 			

Project #3				Contact	
Company Name:	California Department of Public Health			Contact Name & Role:	Ian Sanford, Security Architect
Project Name:	CalCONNECT			Company/Org Name:	California Department of Public
Start Date (MM/DD/YYYY):	4/1/2022	End Date:	7/30/2024	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	33%	Email:	

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities developing, implementing, improving, and monitoring industry-standard security strategies, solutions, and processes on projects involving an AWS cloud environment include:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Develops, implements, improves, and monitors industry-standard security strategies, solutions, and processes on CalCONNECT's large, complex IT systems, including Salesforce and AWS cloud environments • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture • Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments via dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management • Creates, manages, and updates the CalCONNECT project's System Security Plan (SSP) that contains the project's security controls and procedures • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments. • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors. <p>Reporting</p> <ul style="list-style-type: none"> • Maintains IS strategy (forward-looking roadmap), aligning services to the strategy. • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk. • Responds promptly to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification. <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan. • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training after project onboarding/roll-on. • Created, updates, and manages the CalCONNECT project's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the myCAvax solution. • Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations
Project #4	
Company Name:	Contact
California Department of Public Health	Contact Name & Role: Ian Sanford, Security Architect

Project Name:	myCAvax			Company/Org Name:	California Department of Public
Start Date (MM/DD/YYYY):	12/1/2020	End Date (MM/DD/YYYY):	3/31/2022	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	50%	Email:	
	<p>As the Security Manager, Ben's accomplishments and responsibilities developing, implementing, improving, and monitoring strategies, solutions, and processes on projects involving an AWS cloud environment included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Develops, implements, improves, and monitors industry-standard security strategies, solutions, and processes on the Vaccine Management Program's large, complex IT systems, including Salesforce and AWS cloud environments • Responsible for development and deployment of cybersecurity solutions, protection of personal information, digital information, and security compliance • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture • Led the design, development, and implementation of a DevSecOps solution for the Vaccine Management solution's Salesforce application that includes scanning of application code in AWS environments via dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Identifies information security weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the Vaccine Management Program's plans and procedures for business continuity and security incident management • Created, manages, and updates the Vaccine Management Program's System Security Plan that contains the project's security controls and procedures • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from vaccine hunters, Twitter 				

Description of relevant experience:	bots, and malicious threat actors to protect vaccines when supply was limited			
	<p>Reporting</p> <ul style="list-style-type: none"> • Maintains IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds timely to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training after project onboarding/roll-on • Created, updates, and manages the Vaccine Management Program's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the CalCONNECT solution • Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations 			
Project #5				Contact
Company Name:	California Department of Public Health			Contact Name & Role: Ian Sanford, Security Architect
Project Name:	CalCONNECT			Company/Org Name: California Department of Public Health
Start Date (MM/DD/YYYY):	12/1/2020	End Date:	3/31/2022	Phone Number:
Staff Role:	Security Manager	Percentage of Time:	50%	Email:

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities developing, implementing, improving, and monitoring industry-standard security strategies, solutions, and processes on projects involving an AWS cloud environment included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Develops, implements, improves, and monitors industry-standard security strategies, solutions, and processes on CalCONNECT's large, complex IT systems, including Salesforce and AWS cloud environments • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture • Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments via dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management • Creates, manages, and updates the CalCONNECT project's System Security Plan (SSP) that contains the project's security controls and procedures • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments. • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors. <p>Reporting</p> <ul style="list-style-type: none"> • Maintains IS strategy (forward-looking roadmap), aligning services to the strategy. • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk. • Responds promptly to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification. <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan. • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training after project onboarding/roll-on. • Created, updates, and manages the CalCONNECT project's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the myCAvax solution. • Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations
Project #6	
Contact	
<p>Company Name:</p>	<p>California Department of Public Health</p>
<p>Contact Name & Role:</p>	<p>Ian Sanford, Security Architect</p>

Project Name:	CalCONNECT			Company/Org Name:	California Department of Public
Start Date (MM/DD/YYYY):	6/1/2020	End Date:	11/30/2020	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	100%	Email:	
Description of relevant experience:	<p>As the Security Manager, Ben's accomplishments and responsibilities developing, implementing, improving, and monitoring strategies, solutions, and processes on projects involving an AWS cloud environment included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Develops, implements, improves, and monitors industry-standard security strategies, solutions, and processes on CalCONNECT's large, complex IT systems, including Salesforce and AWS cloud environments • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture • Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments via dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management • Creates, manages, and updates the CalCONNECT project's System Security Plan (SSP) that contains the project's security controls and procedures • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments. • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors. <p>Reporting</p> <ul style="list-style-type: none"> • Maintains IS strategy (forward-looking roadmap), aligning services to the strategy. • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk. • Responds promptly to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification. <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan. • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training after project onboarding/roll-on. • Created, updates, and manages the CalCONNECT project's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the myCAVax solution. • Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations 				

Project #7				Contact	
Company Name:	California Office of Systems Integration, Covered California			Contact Name & Role:	Thea Man; Deputy Chief Information Security Officer
Project Name:	California Healthcare Eligibility, Enrollment, and Retention System (CalHEERS)			Company/Org Name:	California Office of Systems Integration, Covered California
Start Date (MM/DD/YYYY):	3/1/2014	End Date:	5/31/2020	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	100%	Email:	
<p>As the Security Manager, Ben's accomplishments and responsibilities developing, implementing, improving, and monitoring industry-standard security strategies, solutions, and processes on projects involving an AWS cloud environment included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Led the development, implementation, improvement, and ongoing monitoring of industry-standard security strategies, solutions, and processes using COTS applications, such as Oracle and GetInsured, on CalHEERS • Developed, implemented and managed the CalHEERS project's application security testing program, which included scans of application code in AWS-hosted development and test environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Implemented, maintained, and managed the security solutions for the CalHEERS project's archived data storage and development and test environments that were hosted in the CalHEERS AWS cloud and on-premises data centers • Conducted information security risk assessment and privacy impact assessments annually • Validated security controls and processes via annual security control reviews in accordance with the Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E) standards, and reviewed results of reviews and recommendations with Covered California's CISO and Security Architect • Managed and tracked security gaps identified during assessments using the federal POA&M process • Developed and deployed complex IAM solutions using the Oracle Identity and Access Management (IAM) platform for self-service registration, user provisioning, application authentication, and single sign-on with enterprise credentials • Enabled the provisioning and secure management of more than 20,000 internal users, 10 million Californians, and 100,000 concurrent users, meeting availability requirements of 98% • Reviewed and maintained security measures, recommended actions, and implemented enhancements • Created, updated, and managed the CalHEERS project's System Security Plan, technical design documents and operational manuals for security tools, security architecture diagrams, and incident management procedures • Managed the application security testing program, which included scans of application code using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) 					

Description of relevant experience:

Reporting

- Led a Security team that managed security devices and responded to security events/incidents, including timely notification of incidents to the CISO and Security Architect in accordance with the CalHEERS project's requirements for security incident notification
- Conducted routine weekly scanning of servers using the project's Qualys solution to identify and rank vulnerabilities delivered in summary and detailed reports, so CalHEERS project leadership could prioritize remediation actions according to vulnerability threat and potential impact levels
- Designed and conducted vulnerability and penetration testing to identify and test methods for exploiting vulnerabilities to circumvent or defeat the security features of the system and supporting infrastructure and provide recommendations for remediation and mitigation to the Covered California CISO and Security Architect
- **Supported the CalHEERS infrastructure, including assembling, configuring, and running various tests, such as manual and automated attack methods for penetration testing**
- Collaborated with a partner to manage a Security team that managed security devices and responded to security events/incidents.

Compliance

- Adhered to security compliance and privacy requirement standards, including the CMS MARS-E; PPACA; IRS Publication 1075 Tax Information Security Guidelines for federal, State, and local agencies; and State of California privacy requirements
- **Collaborated with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments**
- Created, updated, and managed the CalHEERS project's plans and procedures for disaster recovery and business continuity, and led the execution of restores for the CalHEERS system's data centers
- Built a comprehensive security program that aligned to standards from the FISMA and the NIST 800-37 Risk Management Framework
- **Implemented, maintained, and enforced the security and compliance standards, regulations, policies, and frameworks to protect PII, PHI, and FTI data:**
 - NIST 800-53: Security and Privacy Controls for Information Systems Organizations that confirms delivery of information security services follows applicable standards and regulatory requirements
 - Federal Information Processing Standard Publication 199
 - California Statewide Information Management Manual (SIMM)
 - California State Administrative Manual (SAM)
 - MARS-E, Versions 1.0 and 2.0: Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
 - HIPAA regulatory standards

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE					
Contractor -	Accenture		Candidate Name -	Ben Trogia	
Minimum Qualification - S33	A minimum of three (3) years of experience within the past ten (10) years applying Information Security principles, methods, and techniques in the development of Project security Deliverables.				
Project Name	Start Date	End Date	Percentage of Time	Duration in Months	Project Value
CalSAWS	4/1/2022	7/30/2024	34%	28.0	9.5
myCAvax	4/1/2022	7/30/2024	33%	28.0	9.2
CalCONNECT	4/1/2022	7/30/2024	33%	28.0	9.2
myCAvax	12/1/2020	3/31/2022	50%	16.0	8.0
CalCONNECT	12/1/2020	3/31/2022	50%	16.0	8.0
CalCONNECT	6/1/2020	11/30/2020	100%	6.0	6.0
California Healthcare Eligibility, E	3/1/2014	5/31/2020	100%	75.0	75.0
Totals				196.9	124.9

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS PROJECT DETAILS					
Minimum Qualification - S33	A minimum of three (3) years of experience within the past ten (10) years applying Information Security principles, methods, and techniques in the development of Project security Deliverables.				
Project #1			Contact		
Company Name:	CalSAWS Consortium		Contact Name & Role:	Michele Peterson, Test/Release Manager Section Director	
Project Name:	CalSAWS		Company/Org Name:	CalSAWS Consortium	
Start Date (MM/DD/YYYY):	4/1/2022	End Date (MM/DD/YYYY):	7/30/2024	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	34%	Email:	

As the Security Manager, Ben's accomplishments and responsibilities applying information security principles, methods, and techniques in the development of project security deliverables include:

Solution development

- Oversees a Security team of 42 professionals (14 onshore, 28 offshore)
- Collaborates with Application Development teams, technical architects, the CalSAWS Security Operations Lead, and the CalSAWS Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the CalSAWS environment and data
- For each solution we introduced at CalSAWS, **created deliverables and updated project documentation**
- Designed, built, implemented, and operated a Qualys Endpoint Detection and Response (EDR) solution on all Windows and Linux servers, CalSAWS workstations, and County-managed workstations—12,000 devices
- Delivered CalSAWS greater value by switching licenses while heightening the security posture through the EDR solution
- Designed, built, implemented, and operated a file integrity monitoring solution for CalSAWS Linux and Windows servers
- After we enabled AWS Inspector, reviewed the security findings for the Lambda functions, then coordinated and organized the findings with the Application Development teams
- Architected, designed, and built different security solution for Open Plan of Action and Milestones (POAMS)
- Collaborated with the CalSAWS privacy officer, CalSAWS ISO, and CalSAWS Security team to present the POAMS solutions
- Led team that performed the architecture analysis and solution development to move CalSAWS' security posture from NIST 800-53 Rev 4 to Rev 5
- Collaborated with the CalSAWS privacy officer, CalSAWS ISO, and CalSAWS Security team to detail the NIST 800-53 Rev 5 solution
- Assisted Linux and Windows team architects on implementing the CIS security standards to harden workstations that required detailed knowledge of the scripts
- **Applies security principles, methods, and techniques** including **segregation of duties, confidentiality, and least privilege when developing project security deliverables**

Description of relevant experience:	security deliverables <ul style="list-style-type: none"> • Supports key project security deliverables including providing bi-weekly security status updates that involve sharing the progress of key findings, initiatives, and milestones across the range of security services we support—like incident response, compliance, endpoint detection and response, threat and vulnerability management, and application security • Supports periodic review and updates of the operational working documents (OWDs) for each of the project security deliverable processes • Verifies appropriate personnel are supporting the project security deliverable processes on a need-to-know basis or key cybersecurity capabilities • Applies segregation of duties to validate that operational personnel can support the technical tasks needed to be performed 				
	Reporting <ul style="list-style-type: none"> • Maintains IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds promptly to security events/incidents and provides timely notification of incidents to the CalSAWS Security Operations Lead and the CalSAWS Privacy Officer of incidents, in accordance with requirements for security incident notification 				
	Compliance <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training following project onboarding/roll-on • Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations 				
Project #2					
Company Name:				California Department of Public Health	
Project Name:				myCAvax	
Start Date:		4/1/2022		End Date (MM/DD/YYYY):	
Staff Role:		Security Manager		Percentage of Time:	
				7/30/2024	
				33%	
Contact Name & Role:				Ian Sanford, Security Architect	
Company/Org Name:				California Department of Public Health	
Phone Number:					
Email:					

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities applying information security principles, methods, and techniques in the development of project security deliverables include:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Applies information security principles, methods, and techniques in the development of project security deliverables, including the Vaccine Management Program's System Security Plan that contains the project's security controls and procedures, the Disaster Recovery Plan, Security Incident Response Management Plan, Technical Design Documents and Operational Manuals for security tools, and security architecture diagrams that are updated annually • Led the design, development, and implementation of a DevSecOps solution for the Vaccine Management solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Identifies information security weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the Vaccine Management Program's plans and procedures for business continuity and security incident management • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from vaccine hunters, Twitter bots, and malicious threat actors to protect vaccines when supply was limited • Collaborates with Application Development teams, technical architects, and the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the Vaccine Management Program environment and data <p>Reporting</p> <ul style="list-style-type: none"> • Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds promptly to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training upon project onboarding/roll-on • Created, updates, and manages the Vaccine Management Program's Disaster Recovery Plan containing the procedures for disaster recovery, and leads the execution of partial and full recoveries of the CalCONNECT solution • Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations
---	--

Project #3				Contact	
Company Name:	California Department of Public Health			Contact Name & Role:	Ian Sanford, Security Architect
Project Name:	CalCONNECT			Company/Org Name:	California Department of Public
Start Date (MM/DD/YYYY):	4/1/2022	End Date:	7/30/2024	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	33%	Email:	
As the Security Manager, Ben's accomplishments and responsibilities applying information security principles, methods, and development of project security deliverables include:					
Solution development <ul style="list-style-type: none">• Applies information security principles, methods, and techniques and leads the development, management and execution of project security deliverables, including CalCONNECT's System Security Plan (SSP) that contains the project's security controls and procedures, the Disaster Recovery Plan, Security Incident Response Management plan, Technical Design Documents and Operational Manuals for security tools, and Security Architecture Diagrams that are updated annually• Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST)• Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments• Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards• Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on• Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management• Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection• Collaborates with client Development, Technical, and Security teams to define and implement information security policies, strategies, procedures, and configurations to confirm confidentiality, integrity, and availability of the client's environment and data• Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors					

Description of relevant experience:	- Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors				
	<p>Reporting</p> <ul style="list-style-type: none"> • Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds timely to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training upon project onboarding/roll-on • Created, updates, and manages the CalCONNECT Disaster Recovery Plan containing the procedures for disaster recovery, and leads the execution of both partial and full recoveries of the myCAVax solution • Implements, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations 				
Project #4				Contact	
Company Name:	California Department of Public Health			Contact Name & Role:	Ian Sanford, Security Architect
Project Name:	myCAVax			Company/Org Name:	California Department of Public
Start Date (MM/DD/YYYY):	12/1/2020	End Date (MM/DD/YYYY):	3/31/2022	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	50%	Email:	

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities applying information security principles, methods, and techniques in the development of project security deliverables included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Applies information security principles, methods, and techniques in the development of project security deliverables, including the Vaccine Management Program's System Security Plan that contains the project's security controls and procedures, the Disaster Recovery Plan, Security Incident Response Management Plan, Technical Design Documents and Operational Manuals for security tools, and security architecture diagrams that are updated annually • Led the design, development, and implementation of a DevSecOps solution for the Vaccine Management solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Identifies information security weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the Vaccine Management Program's plans and procedures for business continuity and security incident management • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from vaccine hunters, Twitter bots, and malicious threat actors to protect vaccines when supply was limited • Collaborates with Application Development teams, technical architects, and the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the Vaccine Management Program environment and data <p>Reporting</p> <ul style="list-style-type: none"> • Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds promptly to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training upon project onboarding/roll-on • Created, updates, and manages the Vaccine Management Program's Disaster Recovery Plan containing the procedures for disaster recovery, and leads the execution of partial and full recoveries of the CalCONNECT solution • Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations
---	---

Project #5				Contact	
Company Name:	California Department of Public Health			Contact Name & Role:	Ian Sanford, Security Architect
Project Name:	CalCONNECT			Company/Org Name:	California Department of Public Health
Start Date (MM/DD/YYYY):	12/1/2020	End Date:	3/31/2022	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	50%	Email:	
	<p>As the Security Manager, Ben's accomplishments and responsibilities applying information security principles, methods, development of project security deliverables included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Applies information security principles, methods, and techniques and leads the development, management and execution of project security deliverables, including CalCONNECT's System Security Plan (SSP) that contains the project's security controls and procedures, the Disaster Recovery Plan, Security Incident Response Management plan, Technical Design Documents and Operational Manuals for security tools, and Security Architecture Diagrams that are updated annually • Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys 				

Description of relevant experience:	<ul style="list-style-type: none"> • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Collaborates with client Development, Technical, and Security teams to define and implement information security policies, strategies, procedures, and configurations to confirm confidentiality, integrity, and availability of the client's environment and data • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors <p>Reporting</p> <ul style="list-style-type: none"> • Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds timely to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training upon project onboarding/roll-on • Created, updates, and manages the CalCONNECT Disaster Recovery Plan containing the procedures for disaster recovery, and leads the execution of both partial and full recoveries of the myCAVax solution • Implements, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations
--	--

Project #6				Contact	
Company Name:		California Department of Public Health		Contact Name & Role:	Ian Sanford, Security Architect
Project Name:		CalCONNECT		Company/Org Name:	California Department of Public Health
Start Date (MM/DD/YYYY):	6/1/2020	End Date:	11/30/2020	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	100%	Email:	

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities applying information security principles, methods, and techniques in the development of project security deliverables included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Applies information security principles, methods, and techniques and leads the development, management and execution of project security deliverables, including CalCONNECT's System Security Plan (SSP) that contains the project's security controls and procedures, the Disaster Recovery Plan, Security Incident Response Management plan, Technical Design Documents and Operational Manuals for security tools, and Security Architecture Diagrams that are updated annually • Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Collaborates with client Development, Technical, and Security teams to define and implement information security policies, strategies, procedures, and configurations to confirm confidentiality, integrity, and availability of the client's environment and data • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors <p>Reporting</p> <ul style="list-style-type: none"> • Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds timely to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training upon project onboarding/roll-on • Created, updates, and manages the CalCONNECT Disaster Recovery Plan containing the procedures for disaster recovery, and leads the execution of both partial and full recoveries of the myCAvax solution • Implements, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations
<p>Project #7</p>	<p>Contact</p>

Company Name:	California Office of Systems Integration, Covered California			Contact Name & Role:	Thea Man; Deputy Chief Information Security Officer
Project Name:	California Healthcare Eligibility, Enrollment, and Retention System (CalHEERS)			Company/Org Name:	California Office of Systems Integration, Covered California
Start Date (MM/DD/YYYY):	3/1/2014	End Date:	5/31/2020	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	100%	Email:	
Description of relevant experience:	<p>As the Security Manager, Ben's accomplishments and responsibilities applying information security principles, methods, development of project security deliverables included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Applied information security principles, methods, and techniques and led the development of project security deliverables, including the CalHEERS System Security Plan that contains the project's security controls and procedures, Security Risk Assessment, and Privacy Impact Assessment that were updated annually • Validated security controls and processes using annual security control reviews in accordance with the Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E) standards, and reviewed results of reviews and recommendations with Covered California's CISO and Security Architect • Led a Security Operations team that managed security devices and responded to security events/incidents • Managed and tracked security gaps identified during assessments and audits using the CalHEERS project's Plan of Action and Milestones (POA&M) process • Developed and deployed complex IAM solutions using the Oracle Identity and Access Management (IAM) platform for self-service registration, user provisioning, application authentication, and single sign-on with enterprise credentials • Enabled the provisioning and secure management of more than 20,000 internal users, 10 million Californians, and 100,000 concurrent users, and met availability requirements of 98% • Reviewed and maintained security measures, recommended actions, and implemented enhancements • Managed the application security testing program, which included scans of application code using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) <p>Reporting</p> <ul style="list-style-type: none"> • Led a Security team that managed security devices and responded to security events/incidents, including timely notification of incidents to the CISO and Security Architect in accordance with the CalHEERS project's requirements for security incident notification • Conducted routine weekly scanning of servers using the project's Qualys solution to identify and rank vulnerabilities delivered in summary and detailed reports, so CalHEERS project leadership could prioritize remediation actions according to vulnerability threat and potential impact levels • Designed and conducted vulnerability and penetration testing to identify and test methods for exploiting vulnerabilities to circumvent or defeat the security features of the system and supporting infrastructure and provide recommendations for remediation and mitigation to the Covered California CISO and Security Architect • Conducted the information security risk assessment and privacy impact assessment for the CalHEERS 				

- Supported the CalHEERS infrastructure, including assembling, configuring, and running various tests, such as manual and automated attack methods and tests for penetration testing

Compliance

- **Adhered to security compliance and privacy requirement standards, including the CMS MARS-E; PPACA; IRS Publication 1075 Tax Information Security Guidelines for federal, State, and local agencies; and State of California privacy requirements**
- Created, updated, and managed the CalHEERS project's System Security Plan, technical design documents and operational manuals for security tools, security architecture diagrams, and security incident management procedures
- Collaborated with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments
- Created, updated, and managed the CalHEERS project's Disaster Recovery Plan containing the procedures for disaster recovery and business continuity, and led the execution of restores for the CalHEERS system's data centers
- **Implemented, maintained, and enforced the security and compliance standards, regulations, policies, and frameworks to protect PII, PHI, and FTI data:**
 - NIST 800-53: Security and Privacy Controls for Information Systems Organizations that confirms delivery of information security services follows applicable standards and regulatory requirements
 - Federal Information Processing Standard Publication 199
 - California Statewide Information Management Manual (SIMM)
 - California State Administrative Manual (SAM)
 - MARS-E, Versions 1.0 and 2.0: Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
 - HIPAA regulatory standards
 - IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies (Safeguards for Protecting Federal Tax Information (FTI))
- Built a comprehensive security program that aligned to standards from the FISMA and the NIST 800-37 Risk Management Framework

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE					
Contractor -	Accenture		Candidate Name - Ben Troglia		
Minimum Qualification - S34	A minimum of three (3) years of experience assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) to identify appropriate security controls to protect Personally Identifiable Information (PII), Protected Health Information (PHI) and/or Federal Tax Information (FTI) data.				
Project Name	Start Date	End Date	Percentage of Time	Duration in Months	Project Value
CalSAWS	4/1/2022	7/30/2024	34%	28.0	9.5
myCAvax	4/1/2022	7/30/2024	33%	28.0	9.2
CalCONNECT	4/1/2022	7/30/2024	33%	28.0	9.2
myCAvax	12/1/2020	3/31/2022	50%	16.0	8.0
CalCONNECT	12/1/2020	3/31/2022	50%	16.0	8.0
CalCONNECT	6/1/2020	11/30/2020	100%	6.0	6.0
California Healthcare Eligibility, Enrollmen	3/1/2014	5/31/2020	100%	75.0	75.0
Totals				196.9	124.9

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS PROJECT DETAILS					
Minimum Qualification - S34	A minimum of three (3) years of experience assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) to identify appropriate security controls to protect Personally Identifiable Information (PII), Protected Health Information (PHI) and/or Federal Tax Information (FTI) data.				
Project #1			Contact		
Company Name:	CalSAWS Consortium		Contact Name & Role:	Michele Peterson, Test/Release Manager Section Director	
Project Name:	CalSAWS		Company/Org Name:	CalSAWS Consortium	
Start Date (MM/DD/YYYY):	4/1/2022	End Date (MM/DD/YYYY):	7/30/2024	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	34%	Email:	

As the Security Manager, Ben's accomplishments and responsibilities assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) to identify appropriate security controls to protect Personally Identifiable Information (PII), Protected Health Information (PHI), and/or Federal Tax Information (FTI) data include:

Solution development

• **Assesses system data sensitivity using security categorizations while identifying and implementing the following security controls to protect PII and PHI:**

- State Administrative Manual (SAM) sections 5300 – 5365.3 (06/2014)
- Statewide Information Management Manual (SIMM) section SIMM 5305-A (01/2018)
- Public Health Administrative Manual (PHAM) Privacy Act
- CDPH Information Systems Security Requirements for Projects (ISO/SR1)
- NIST 800-111 Guide to Storage Encryption Technologies for End User Devices (11/2007)
- NIST 800-88 Guidelines for Media Sanitation (12/2014)
- NIST 800-71 Recommendation for Key Establishment Using Symmetric Block Ciphers (06/2018)
- NIST 800-39 Managing Information Security Risk (03/2011)
- NIST 800-30 Risk Management Guide for Information Technology Systems (09/2012)
- NIST 800-53 Security and Privacy Controls for Information Systems and Organizations
- NIST 800-63 Electronic Authentication Guideline
- FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems (02/2004)
- California Government Code sections 11019.9 and 11549.3 (2010)
- Information Privacy Act (Civil Code section 1798 et seq.)
- Public Records Act (California Gov. Code Section 6250 et seq.)

• **Implements, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:**

- Federal Information Processing Standard Publication 199
- California Statewide Information Management Manual (SIMM)
- California State Administrative Manual (SAM)
- HIPAA regulatory standards
- NIST 800-53: Security and Privacy Controls for Information Systems Organizations

• **Oversees a Security team of 25 professionals (eight onshore, 17 offshore)**

- Collaborates with Application Development teams, technical architects, the CalSAMIS Security Operations Lead, and the CalSAMIS Privacy

Description of relevant experience: <ul style="list-style-type: none"> • Collaborates with Application Development teams, technical architects, the CalSAWS Security Operations Lead, and the CalSAWS Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the CalSAWS environment and data • For each solution we introduced at CalSAWS, created deliverables and updated project documentation • Designed, built, implemented, and operated a Qualys Endpoint Detection and Response (EDR) solution on all Windows and Linux servers, CalSAWS workstations, and County-managed workstations—12,000 devices • Delivered CalSAWS greater value by switching licenses while heightening the security posture through the EDR solution • Designed, built, implemented, and operated a file integrity monitoring solution for CalSAWS Linux and Windows servers • After we enabled AWS Inspector, reviewed the security findings for the Lambda functions, then coordinated and organized the findings with the Application Development teams • Architected, designed, and built different security solution for Open Plan of Action and Milestones (POAMS) • Collaborated with the CalSAWS privacy officer, CalSAWS ISO, and CalSAWS Security team to present the POAMS solutions • Led team that performed the architecture analysis and solution development to move CalSAWS' security posture from NIST 800-53 Rev 4 to Rev 5 • Collaborated with the CalSAWS privacy officer, CalSAWS ISO, and CalSAWS Security team to detail the NIST 800-53 Rev 5 solution • Assisted Linux and Windows team architects on implementing the CIS security standards to harden workstations that required detailed knowledge of the scripts <p>Reporting</p> <ul style="list-style-type: none"> • Maintains IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds promptly to security events/incidents and provides timely notification of incidents to the CalSAWS Security Operations Lead and the CalSAWS Privacy Officer of incidents, in accordance with requirements for security incident notification <p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training following project onboarding/roll-on 						
Project #2				Contact		
Company Name:			California Department of Public Health		Contact Name & Role:	Ian Sanford, Security Architect
Project Name:			myCAvax		Company/Org Name:	California Department of Public Health
Start Date:		4/1/2022	End Date (MM/DD/YYYY):		7/30/2024	Phone Number:
Staff Role:		Security Manager	Percentage of Time:		33%	Email:

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) to identify appropriate security controls to protect Personally Identifiable Information (PII), Protected Health Information (PHI), and/or Federal Tax Information (FTI) data include:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Assesses system data sensitivity using security categorizations while identifying and implementing the following security controls to protect PII and PHI: <ul style="list-style-type: none"> - State Administrative Manual (SAM) sections 5300 – 5365.3 (06/2014) - Statewide Information Management Manual (SIMM) section SIMM 5305-A (01/2018) - Public Health Administrative Manual (PHAM) Privacy Act - CDPH Information Systems Security Requirements for Projects (ISO/SR1) - NIST 800-111 Guide to Storage Encryption Technologies for End User Devices (11/2007) - NIST 800-88 Guidelines for Media Sanitation (12/2014) - NIST 800-71 Recommendation for Key Establishment Using Symmetric Block Ciphers (06/2018) - NIST 800-39 Managing Information Security Risk (03/2011) - NIST 800-30 Risk Management Guide for Information Technology Systems (09/2012) - NIST 800-53 Security and Privacy Controls for Information Systems and Organizations - NIST 800-63 Electronic Authentication Guideline - FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems (02/2004) - California Government Code sections 11019.9 and 11549.3 (2010) - Information Privacy Act (Civil Code section 1798 et seq.) - Public Records Act (California Gov. Code Section 6250 et seq.) • Implements, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations. • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the Vaccine Management Program environment and data • Led the design, development, and implementation of a DevSecOps solution for the Vaccine Management solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Identifies information security weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the Vaccine Management Program's plans and procedures for business continuity and security incident management
---	--

management

- Created, manages, and updates the Vaccine Management Program's System Security Plan that contains the project's security controls and procedures
- Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection
- Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from vaccine hunters, Twitter bots, and malicious threat actors to protect vaccines when supply was limited

Reporting

- Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy
- Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk
- Responds timely to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification

Compliance

- Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan
- Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training upon project onboarding/roll-on
- Created, updates, and manages the Vaccine Management Program's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the CalCONNECT solution

Project #3				Contact	
Company Name:	California Department of Public Health			Contact Name & Role:	Ian Sanford, Security Architect
Project Name:	CalCONNECT			Company/Org Name:	California Department of Public Health
Start Date (MM/DD/YYYY):	4/1/2022	End Date:	7/30/2024	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	33%	Email:	

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) to identify appropriate security controls to protect Personally Identifiable Information (PII), Protected Health Information (PHI), and/or Federal Tax Information (FTI) data include:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Assesses system data sensitivity using security categorizations while identifying and implementing the following security controls to protect PII and PHI: <ul style="list-style-type: none"> - State Administrative Manual (SAM) sections 5300 – 5365.3 (06/2014) - Statewide Information Management Manual (SIMM) section SIMM 5305-A (01/2018) - Public Health Administrative Manual (PHAM) Privacy Act - CDPH Information Systems Security Requirements for Projects (ISO/SR1) - NIST 800-111 Guide to Storage Encryption Technologies for End User Devices (11/2007) - NIST 800-88 Guidelines for Media Sanitation (12/2014) - NIST 800-71 Recommendation for Key Establishment Using Symmetric Block Ciphers (06/2018) - NIST 800-39 Managing Information Security Risk (03/2011) - NIST 800-30 Risk Management Guide for Information Technology Systems (09/2012) - NIST 800-63-3 Electronic Authentication Guideline - FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems (02/2004) - California Government Code sections 11019.9 and 11549.3 (2010) - Information Privacy Act (Civil Code section 1798 et seq.) - Public Records Act (California Gov. Code Section 6250 et seq.) • Implements, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the CalCONNECT environment and data • Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments. • Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management • Created, manages, and updates the CalCONNECT project's System Security Plan (SSP) that contains the project's security controls and procedures • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors
---	---

Reporting

- Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy
- Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk
- Responds promptly to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification

Compliance

- Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan
- Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training after project onboarding/roll-on
- Created, updates, and manages the CalCONNECT project's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the myCAVax solution

Project #4				Contact	
Company Name:	California Department of Public Health			Contact Name & Role:	Ian Sanford, Security Architect
Project Name:	myCAVax			Company/Org Name:	California Department of Public Health
Start Date (MM/DD/YYYY):	12/1/2020	End Date (MM/DD/YYYY):	3/31/2022	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	50%	Email:	
As the Security Manager, Ben's accomplishments and responsibilities assessing system data sensitivity using security Publication 199) to identify appropriate security controls to protect Personally Identifiable Information (PII), Protected Health Information (PHI), and/or Federal Tax Information (FTI) data included:					
Solution development					
• Assesses system data sensitivity using security categorizations while identifying and implementing the following security controls to protect PII and PHI:					
- State Administrative Manual (SAM) sections 5300 – 5365.3 (06/2014)					
- Statewide Information Management Manual (SIMM) section SIMM 5305-A (01/2018)					
- Public Health Administrative Manual (PHAM) Privacy Act					
- CDPH Information Systems Security Requirements for Projects (ISO/SR1)					
- NIST 800-111 Guide to Storage Encryption Technologies for End User Devices (11/2007)					
- NIST 800-88 Guidelines for Media Sanitation (12/2014)					
- NIST 800-71 Recommendation for Key Establishment Using Symmetric Block Ciphers (06/2018)					
- NIST 800-39 Managing Information Security Risk (03/2011)					
- NIST 800-30 Risk Management Guide for Information Technology Systems (09/2012)					
- NIST 800-53 Security and Privacy Controls for Information Systems and Organizations					
- NIST 800-63 Electronic Authentication Guideline					
- FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems (02/2004)					
- California Government Code sections 11019.9 and 11549.3 (2010)					
- Information Privacy Act (Civil Code section 1798 et seq.)					
- Public Records Act (California Gov. Code Section 6250 et seq.)					

Description of relevant experience:	<p>Public Records Act (California Gov. Code Section 6250 et seq.)</p> <ul style="list-style-type: none"> • Implements, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations. • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the Vaccine Management Program environment and data • Led the design, development, and implementation of a DevSecOps solution for the Vaccine Management solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments • Identifies information security weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the Vaccine Management Program's plans and procedures for business continuity and security incident management • Created, manages, and updates the Vaccine Management Program's System Security Plan that contains the project's security controls and procedures • Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection • Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from vaccine hunters, Twitter bots, and malicious threat actors to protect vaccines when supply was limited 		
	<p>Reporting</p> <ul style="list-style-type: none"> • Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds timely to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification 		
	<p>Compliance</p> <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training upon project onboarding/roll-on • Created, updates, and manages the Vaccine Management Program's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the CalCONNECT solution 		
Project #5		Contact	
Company Name:	California Department of Public Health	Contact Name & Role:	Ian Sanford, Security Architect

Project Name:	CalCONNECT			Company/Org Name:	California Department of Public Health
Start Date (MM/DD/YYYY):	12/1/2020	End Date:	3/31/2022	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	50%	Email:	
Description of relevant experience:	<p>As the Security Manager, Ben's accomplishments and responsibilities assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) to identify appropriate security controls to protect Personally Identifiable Information (PII), Protected Health Information (PHI), and/or Federal Tax Information (FTI) data included:</p> <p>Solution development</p> <ul style="list-style-type: none">• Assesses system data sensitivity using security categorizations while identifying and implementing the following security controls to protect PII and PHI:<ul style="list-style-type: none">- State Administrative Manual (SAM) sections 5300 – 5365.3 (06/2014)- Statewide Information Management Manual (SIMM) section SIMM 5305-A (01/2018)- Public Health Administrative Manual (PHAM) Privacy Act- CDPH Information Systems Security Requirements for Projects (ISO/SR1)- NIST 800-111 Guide to Storage Encryption Technologies for End User Devices (11/2007)- NIST 800-88 Guidelines for Media Sanitation (12/2014)- NIST 800-71 Recommendation for Key Establishment Using Symmetric Block Ciphers (06/2018)- NIST 800-39 Managing Information Security Risk (03/2011)- NIST 800-30 Risk Management Guide for Information Technology Systems (09/2012)- NIST 800-63-3 Electronic Authentication Guideline- FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems (02/2004)- California Government Code sections 11019.9 and 11549.3 (2010)- Information Privacy Act (Civil Code section 1798 et seq.)- Public Records Act (California Gov. Code Section 6250 et seq.)• Implements, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:<ul style="list-style-type: none">- Federal Information Processing Standard Publication 199- California Statewide Information Management Manual (SIMM)- California State Administrative Manual (SAM)- HIPAA regulatory standards- NIST 800-53: Security and Privacy Controls for Information Systems Organizations• Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the CalCONNECT environment and data• Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST)• Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments.• Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards• Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on• Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management• Created, manages, and updates the CalCONNECT project's System Security Plan (SSP) that contains the project's security controls and				

procedures

- Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection
- Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors

Reporting

- Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy
- Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk
- Responds promptly to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification

Compliance

- Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan
- Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training after project onboarding/roll-on
- Created, updates, and manages the CalCONNECT project's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the myCAVax solution

Project #6				Contact	
Company Name:	California Department of Public Health			Contact Name & Role:	Ian Sanford, Security Architect
Project Name:	CalCONNECT			Company/Org Name:	California Department of Public Health
Start Date (MM/DD/YYYY):	6/1/2020	End Date:	11/30/2020	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	100%	Email:	

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) to identify appropriate security controls to protect Personally Identifiable Information (PII), Protected Health Information (PHI), and/or Federal Tax Information (FTI) data included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Assesses system data sensitivity using security categorizations while identifying and implementing the following security controls to protect PII and PHI: <ul style="list-style-type: none"> - State Administrative Manual (SAM) sections 5300 – 5365.3 (06/2014) - Statewide Information Management Manual (SIMM) section SIMM 5305-A (01/2018) - Public Health Administrative Manual (PHAM) Privacy Act - CDPH Information Systems Security Requirements for Projects (ISO/SR1) - NIST 800-111 Guide to Storage Encryption Technologies for End User Devices (11/2007) - NIST 800-88 Guidelines for Media Sanitation (12/2014) - NIST 800-71 Recommendation for Key Establishment Using Symmetric Block Ciphers (06/2018) - NIST 800-39 Managing Information Security Risk (03/2011) - NIST 800-30 Risk Management Guide for Information Technology Systems (09/2012) - NIST 800-63-3 Electronic Authentication Guideline - FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems (02/2004) - California Government Code sections 11019.9 and 11549.3 (2010) - Information Privacy Act (Civil Code section 1798 et seq.) - Public Records Act (California Gov. Code Section 6250 et seq.) • Implements, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations • Collaborates with Application Development teams, technical architects, the CDPH Security Operations Lead, and the CDPH Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the CalCONNECT environment and data • Led the design, development, and implementation of a DevSecOps solution for the CalCONNECT solution's Salesforce application that includes scanning of application code in AWS environments using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) • Collaborates with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments. • Identifies information security (IS) weaknesses or potential gaps in the current environment and collaborates with the client Security team to bring information security operations up to standards • Managed the design, development, and implementation of an access control solution using Microsoft Azure single sign-on • Developed and implemented the CalCONNECT project's plans and procedures for business continuity and security incident management
---	---

- Created, manages, and updates the CalCONNECT project's System Security Plan (SSP) that contains the project's security controls and procedures
- Evaluates new/emerging security products and technologies and makes recommendations for adoption to CDPH executives, such as the Qualys solution for vulnerability management, policy compliance, and file integrity monitoring and web application firewalls/bot management protection
- Architected and deployed a complex bot management solution to protect California's COVID-19 contact tracing systems from malicious threat actors

Reporting

- Maintains the IS strategy (forward-looking roadmap), aligning services to the strategy
- Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk
- Responds promptly to security events/incidents and provides timely notification of incidents to the CDPH Security Operations Lead and the CDPH Privacy Officer of incidents, in accordance with requirements for security incident notification

Compliance

- Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan
- Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training after project onboarding/roll-on
- Created, updates, and manages the CalCONNECT project's plans and procedures for disaster recovery, and leads the execution of partial and full recoveries of the myCAVax solution

Project #7				Contact	
Company Name:	California Office of Systems Integration, Covered California			Contact Name & Role:	Thea Man; Deputy Chief Information Security Officer
Project Name:	California Healthcare Eligibility, Enrollment, and Retention System (CalHEERS)			Company/Org Name:	California Office of Systems Integration, Covered California
Start Date (MM/DD/YYYY):	3/1/2014	End Date:	5/31/2020	Phone Number:	
Staff Role:	Security Manager	Percentage of Time:	100%	Email:	

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) to identify appropriate security controls to protect Personally Identifiable Information (PII), Protected Health Information (PHI), and/or Federal Tax Information (FTI) data included:</p> <p>Solution development</p> <ul style="list-style-type: none"> Assessed system data sensitivity using security categorizations while identifying and implementing the CMS MARS-E and IRS Publication 1075 security controls to protect PII, PHI, and FTI data using <ul style="list-style-type: none"> Implemented, maintained, and enforced the security and compliance standards, regulations, policies, and frameworks to protect PII, PHI, and FTI data: <ul style="list-style-type: none"> NIST 800-53: Security and Privacy Controls for Information Systems Organizations that confirms delivery of information security services follows applicable standards and regulatory requirements Federal Information Processing Standard Publication 199 California Statewide Information Management Manual (SIMM) California State Administrative Manual (SAM) MARS-E, Versions 1.0 and 2.0: Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges HIPAA regulatory standards IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies (Safeguards for Protecting Federal Tax Information (FTI)) Security compliance and privacy requirements for this project also factored in these standards: CMS MARS-E and ACA Patient Protection and Affordable Care Act Led a Security Operations team that managed security devices and responded to security events/incidents Conducted information security risk assessment and privacy impact assessment for the CalHEERS Validated security controls and processes using annual security control reviews in accordance with the Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E) standards, and reviewed results of reviews and recommendations with Covered California's CISO and Security Architect Managed and tracked security gaps identified during assessments and audits using the CalHEERS project's Plan of Action and Milestones (POA&M) process Developed and deployed complex identity and access management (IAM) solutions using the Oracle Identity and Access Management (IAM) platform for self-service registration, user provisioning, application authentication, and single sign-on with enterprise credentials Enabled the provisioning and secure management of more than 20,000 internal users, 10 million citizens, and 100,000 concurrent users and met availability requirements of 99%
--	---

Description of relevant experience:

met availability requirements of 98%

- Reviewed and maintained security measures, recommended actions, and implemented enhancements
- Created, updated, and managed the CalHEERS project's System Security Plan, technical design documents and operational manuals for security tools, security architecture diagrams, and security incident management procedures
- Managed the application security testing program, which included scans of application code using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST)

Reporting

- Led a Security team that managed security devices and responded to security events/incidents, including timely notification of incidents to the CISO and Security Architect in accordance with the CalHEERS project's requirements for security incident notification
- Conducted routine weekly scanning of servers using the project's Qualys solution to identify and rank vulnerabilities delivered in summary and detailed reports, so CalHEERS project leadership could prioritize remediation actions according to vulnerability threat and potential impact levels
- Designed and conducted vulnerability and penetration testing to identify and test methods for exploiting vulnerabilities to circumvent or defeat the security features of the system and supporting infrastructure and provide recommendations for remediation and mitigation to the Covered California CISO and Security Architect
- Supported the CalHEERS infrastructure, including assembling, configuring, and running various tests, such as manual and automated attack methods

Compliance

- Adhered to security compliance and privacy requirement standards, including the CMS MARS-E; PPACA; IRS Publication 1075 Tax Information Security Guidelines for Federal, State, and Local Agencies; and State of California privacy requirements
- Collaborated with the Application Development, Technical, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments
- Created, updated, and managed the CalHEERS project's plans and procedures for disaster recovery and business continuity and led the execution of restores for the CalHEERS data centers
- Built a comprehensive security program that aligned to standards from the FISMA, the NIST 800-37 Risk Management Framework and 800-53 System Security Plan controls, and IRS Safeguard Procedures.

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE					
Contractor -	Accenture		Candidate Name -	Ben Troglia	
Minimum Qualification - S35	A minimum of three (3) years of experience with systems that comply with NIST 800-53 moderate baseline.				
Project Name	Start Date	End Date	Percentage of Time	Duration in Months	Project Value
CalSAWS	4/1/2022	7/30/2024	34%	28.0	9.5
California Healthcare Eligibility, Enrollment	3/1/2014	5/31/2020	100%	75.0	75.0
			0%	0.0	0.0
			0%	0.0	0.0
			0%	0.0	0.0
			0%	0.0	0.0
Totals				103.0	84.5

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS PROJECT DETAILS					
Minimum Qualification - S35		A minimum of three (3) years of experience with systems that comply with NIST 800-53 moderate baseline.			
Project #1				Contact	
Company Name:		CalSAWS Consortium		Contact Name & Role:	Michele Peterson, Test/Release Manager Section Director
Project Name:		CalSAWS		Company/Org Name:	CalSAWS Consortium
Start Date (MM/DD/YYYY):		4/1/2022	End Date (MM/DD/YYYY):	7/30/2024	Phone Number:
Staff Role:		Security Manager	Percentage of Time:	34%	Email:
		As the Security Manager, Ben’s accomplishments and responsibilities with systems that comply with NIST 800-53 moderate baseline include: Solution development <ul style="list-style-type: none">• Oversees a Security team of 42 professionals (14 onshore, 28 offshore)• Collaborates with Application Development teams, technical architects, the CalSAWS Security Operations Lead, and the CalSAWS Privacy Officer to define and implement an integrated framework of security solution architecture that includes information security policies, strategies, procedures, and configurations to promote confidentiality, integrity, and availability of the CalSAWS environment and data• Verified that CalSAWS complied with the NIST 800-53 moderate baseline• Led team that performed the architecture analysis and solution development to move CalSAWS' security posture from NIST 800-53 Rev 4 to Rev 5• Collaborated with the CalSAWS privacy officer, CalSAWS ISO, and CalSAWS Security team to detail the NIST 800-53 Rev 5 solution• After we enabled AWS Inspector, reviewed the security findings for the Lambda functions, then coordinated and organized the findings with the Application Development teams• Architected, designed, and built different security solution for Open Plan of Action and Milestones (POAMS)• Collaborated with the CalSAWS privacy officer, CalSAWS ISO, and CalSAWS Security team to present the POAMS solutions• Assisted Linux and Windows team architects on implementing the CIS security standards to harden workstations that required detailed knowledge of the scripts			

Description of relevant experience:	Reporting <ul style="list-style-type: none"> • Maintains IS strategy (forward-looking roadmap), aligning services to the strategy • Monitors the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and makes timely adjustments and/or recommendations to reduce risk • Responds promptly to security events/incidents and provides timely notification of incidents to the CalSAWS Security Operations Lead and the CalSAWS Privacy Officer of incidents, in accordance with requirements for security incident notification 			
	Compliance <ul style="list-style-type: none"> • Confirms delivery of information security services follows applicable standards and regulatory requirements (such as applicable NIST 800-53 controls) and is in accordance with the project's approved System Security Plan • Conducts ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Salesforce development security training following project onboarding/roll-on • Implemented, maintains, and enforces the security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - HIPAA regulatory standards - NIST 800-53: Security and Privacy Controls for Information Systems Organizations 			
Project #2				
Company Name:			California Office of Systems Integration, Covered California	
Project Name:			California Healthcare Eligibility, Enrollment, and Retention System (CalHEERS)	
Start Date:			3/1/2014	End Date:
Staff Role:			Security Manager	Percentage of Time:
			5/31/2020	Phone Number:
			100%	Email:

<p>Description of relevant experience:</p>	<p>As the Security Manager, Ben's accomplishments and responsibilities with systems that comply with NIST 800-53 moderate baseline included:</p> <p>Solution development</p> <ul style="list-style-type: none"> • Worked with CalHEERS which complies with NIST 800-53 moderate baseline • Conducted an information security risk assessment and privacy impact assessments annually • Built a comprehensive security program that aligned to standards from the FISMA, the NIST 800-37 Risk Management Framework and 800-53 System Security Plan controls, and IRS Safeguard Procedures • Created, updated, and managed the CalHEERS project's System Security Plan, technical design documents and operational manuals for security tools, security architecture diagrams, and incident management procedures • Validated security controls and processes using annual security control reviews in accordance with the Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E) standards, and reviewed results of reviews and recommendations with Covered California's CISO and Security Architect • Managed and tracked security gaps identified during assessments and audits using the CalHEERS project's Plan of Action and Milestones (POA&M) process • Led a Security team that managed security devices and responded to security events/incidents, including timely notification of incidents to the CISO and Security Architect in accordance with the CalHEERS project's requirements for security incident notification • Developed and deployed complex IAM solutions using the Oracle Identity and Access Management (IAM) platform for self-service registration, user provisioning, application authentication, and single sign-on with enterprise credentials • Enabled the provisioning and secure management of more than 20,000 internal users, 10 million Californians, and 100,000 concurrent users and met availability requirements of 98% • Reviewed and maintained security measures, recommended actions, and implemented enhancements • Managed the application security testing program, which included scans of application code using dynamic application security testing (DAST), static application security testing (SAST), and interactive application security testing (IAST) <p>Reporting</p> <ul style="list-style-type: none"> • Conducted routine weekly scanning of servers using the project's Qualys solution to identify and rank vulnerabilities delivered in summary and detailed reports so CalHEERS project leadership could prioritize remediation actions according to vulnerability threat and potential impact levels • Designed and conducted vulnerability and penetration testing to identify and test methods for exploiting vulnerabilities to circumvent or defeat the security features of the system and supporting infrastructure and provide recommendations for remediation and mitigation to the Covered California CISO and Security Architect • Supported the CalHEERS infrastructure, including assembling, configuring, and running various tests such as manual and automated attack methods for penetration testing <p>Compliance</p> <ul style="list-style-type: none"> • Adhered to security compliance and privacy requirement standards, including the CMS MARS-E; PPACA; IRS Publication 1075 Tax Information Security Guidelines for federal, State, and local agencies; and State of California privacy requirements • Implemented, maintained, and enforced the security and compliance standards, regulations, policies, and frameworks to protect PII, PHI, and FTI data: <ul style="list-style-type: none"> - NIST 800-53: Security and Privacy Controls for Information Systems Organizations that confirms delivery of information security services follows applicable standards and regulatory requirements - Federal Information Processing Standard Publication 199 - California Statewide Information Management Manual (SIMM) - California State Administrative Manual (SAM) - MARS-E, Versions 1.0 and 2.0: Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges - HIPAA regulatory standards - IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies (Safeguards for Protecting Federal Tax Returns and Return Information)
---	--

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE				
Contractor -	Accenture	Candidate Name - Ben Trogia		
Minimum Qualification - S36	Hold an (ISC)2® Certified Information Systems Security Professional (CISSP) certification, or ISACA Certified Information Security Manager (CISM) and maintain for the duration of the contract.			
Certification/Degree Title	Certification Number	Original Grant Date	Expiration Date	Online Validation Link, if not available attach a copy to the offer
(ISC)2 Certified Information Systems Security Professional (CISSP)	461611	4-Apr-14	30-Apr-25	https://www.isc2.org/MemberVerification