

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	Deloitte Consulting LLP	Candidate Name	Karthik Krishnamurthy
Position in the Company	Senior Manager	Length of Time in Position	25 months
Project Position & Responsibilities	As the Security Manager of BenefitsCal, Karthik's oversees and manages the entire security lifecycle of the project. With the objective to minimize security risks to BenefitsCal operations, Karthik maintains daily operations, researches future designs and risks, and monitors the security controls according to the relevant security standards and requirements and leading practices. Additionally, Karthik leads the security standards, procedures and playbooks that comply with the industry standards and the privacy and security agreements of the project. He operates as the project's security expert for the project and help develop, adopt, and enforce the information security policies, procedures and standards. Karthik keeps the consortium aware and up to date, establishing open lines of communication with the project stakeholders, sharing potential security incidents or breaches. He coordinates with the stakeholders to respond to any security-related data calls, audits, or reports and leads a team of security engineers to perform continuous security monitoring of the systems and identify and mitigate any security weaknesses, threats, or vulnerabilities.		
Skills & Qualifications for Project Position	Karthik exceeds all skills, qualifications, and requirements for this project position. He is a Certified Information Systems Security Professional (CISSP) and has more than 14 years of experience as a Security Manager, working closely with various project teams and stakeholders to establish, design, implement, and monitor security controls in alignment with leading security standards such as NIST 800-53. He was responsible for the security architecture design and implementation of the BenefitsCal solution, and he constantly evaluated and enhanced its security posture based on emerging security threats. He has a strong background in assessing and categorizing system security according to FIPS 199 security standards and developing and maintaining security deliverables such as SSP, POA&M, and security incident response playbooks following best security practices and principles. He has proven leadership skills in managing security incident response activities and leading security teams for continuous security control testing and improvement.		
Education (add rows as needed)			
Start	End	Degree / Course of Study	School
9/1/2014	6/1/2016	Master of Science, Information Management	University of Washington, Seattle
8/1/2004	4/1/2008	Bachelor of Engineering, Electronic and Communication Engineering	Anna University, India
Professional Certifications or Designations (add rows as needed)			
Certification or Designation	Organization	Dates	
Certified Information Systems Security Professional (CISSP)	International Information System Security Certification Consortium (ISC)2	04/01/2024-03/31/2027	
Project Management Professional (PMP)	Project Management Institute (PMI)	04/19/2019-04/19/2025	

Additional Relevant Experience (Add additional tables as needed)				
Project Title #1				
Position Title				
Begin Date		End Date	# of Months	0.0
Scope and Description of Responsibility				
Skills Utilized and Experience Attained				
Project Title #2				
Position Title				
Begin Date		End Date	# of Months	0.0
Scope and Description of Responsibility				
Skills Utilized and Experience Attained				

Project Title #3					
Position Title					
Begin Date		End Date		# of Months	0.0
Scope and Description of Responsibility					
Skills Utilized and Experience Attained					
Project Title #4					
Position Title					
Begin Date		End Date		# of Months	0.0
Scope and Description of Responsibility					
Skills Utilized and Experience Attained					

Project Title #5					
Position Title					
Begin Date		End Date		# of Months	0.0
Scope and Description of Responsibility					
Skills Utilized and Experience Attained					

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE					
Contractor -	Deloitte Consulting LLP		Candidate Name - Karthik Krishnamurthy		
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 - BenefitsCal Maintenance and Enhancement (M&E)	1/6/2022	7/30/2024	50%	30.8	15.4
Security Engineering Improvements	1/6/2022	7/30/2024	50%	30.8	15.4
CalSAWS - BenefitsCal Implementation	8/6/2020	1/5/2022	100%	17.0	17.0
Federal Draw Reporting (FDR) Solution Implementation Project	12/2/2019	8/5/2020	100%	8.1	8.1
Integrated Eligibility (IE) System Security Management	8/1/2016	12/1/2019	100%	40.0	40.0
			0%	0.0	0.0
			Totals	126.7	95.9

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:	California Statewide Automated Welfare System (CalSAWS)		Contact Name & Role:	Joseph Nelson, Chief Privacy Officer	
Project Name:	CalSAWS - BenefitsCal Maintenance and Enhancement (M&E)		Company/Org Name:	CalSAWS Consortium	
Start Date (MM/DD/YYYY):	1/6/2022	End Date (MM/DD/YYYY):	7/30/2024	Phone Number:	[REDACTED]
Staff Role:	Security Lead and Architect	Percentage of Time:	50%	Email:	[REDACTED]
Description of relevant experience:	As the Security Lead and Architect, Karthik led and managed all the security aspects of BenefitsCal system development, maintenance, and operations on a cloud-based AWS platform. His responsibilities included review and monitoring of application and AWS cloud infrastructure security controls in compliance with NIST 800-53, and CalSAWS security standards. Throughout the project, Karthik worked with application development teams, technology architects, Consortium Security and vendor teams to implement and maintain security controls based on the BenefitsCal security architecture.				
Project #2			Contact		
Company Name:	Department of Health Care Services (DHCS)		Contact Name & Role:	Chris Bailey, Chief Information Security Officer	
Project Name:	Security Engineering Improvements		Company/Org Name:	DHCS	
Start Date:	1/6/2022	End Date:	7/30/2024	Phone Number:	[REDACTED]
Staff Role:	Security Project Manager and Architect	Percentage of Time:	50%	Email:	[REDACTED]
Description of relevant experience:	Karthik worked directly with the DHCS CISO, security architects, development team, and cloud infrastructure team to identify security priorities and initiatives to help the overall program. Karthik led a team of security engineers to develop, implement, monitor, and improve security capabilities and controls to meet the NIST 800-53 Rev 5 standard. The security projects delivered to the client included defining and implementing Data Loss Prevention (DLP) capabilities, AWS cloud infrastructure security controls, ransomware preparedness assessment, ServiceNow implementation of Continuous Authorization Module (CAM) with the objective to develop and maintain SSPs, POA&Ms, migration and integration of custom applications with Azure Entra ID for authentication and Multi-Factor Authentication (MFA) enablement, security architecture design based on integrated control framework, network security enhancements, GenAI Governance frameworks, security incident response table top exercises, Active Directory improvement initiatives, and network security improvements.				

Project #3				Contact	
Company Name:	California Statewide Automated Welfare System (CalSAWS)			Contact Name & Role:	Joseph Nelson, Chief Privacy Officer
Project Name:	CalSAWS - BenefitsCal Implementation			Company/Org Name:	CalSAWS Consortium
Start Date (MM/DD/YYYY):	8/6/2020	End Date:	1/5/2022	Phone Number:	
Staff Role:	Project Manager and Information Security Assessment Lead	Percentage of Time:	100%	Email:	
Description of relevant experience:	As the Security Lead and Architect, Karthik led and managed all the security aspects of BenefitsCal system development, maintenance, and operations on a cloud-based AWS platform. His responsibilities included review and monitoring of application and AWS cloud infrastructure security controls in compliance with NIST 800-53, and CalSAWS security standards. Throughout the project, Karthik worked with application development teams, technology architects, Consortium Security and vendor teams to implement and maintain security controls based on the BenefitsCal security architecture.				

  

Project #4				Contact	
Company Name:	Department of Health Care Services (DHCS)			Contact Name & Role:	Richard Green, Chief, Cybersecurity Risk & Compliance Section
Project Name:	Federal Draw Reporting (FDR) Solution Implementation Project			Company/Org Name:	DHCS
Start Date (MM/DD/YYYY):	12/2/2019	End Date:	8/5/2020	Phone Number:	
Staff Role:	Security Architect	Percentage of Time:	100%	Email:	
Description of relevant experience:	As the Security Architect, Karthik led a team responsible for reviewing the requirements, identifying and implementing the security controls based on integrated control framework from applicable security standards. Working with the different teams including development team, technical architects, cloud infrastructure team, DHCS ISO Team for implementation, and performing information security evaluation and compliance of the FDR Solution. Karthik attained the experience of leading the team to design and implement security controls, develop the FDR System Security Plan (SSP) that provides an overview of the security and privacy requirements of the enterprise systems and described the controls in place or planned to improve the protection of information system resources. Karthik also gained experience in conducting periodic security reviews of the FDR Solution with the Department of Health Care Services (DHCS) Information Security Office (ISO) and oversaw the security testing activities and evaluation of compliance of FDR Solution with DHCS Security and Privacy policies, FedRAMP, NIST Special Publication 800-53 (current version), SAM, SIMM, and HIPAA.				

  

Project #5				Contact	
Company Name:	State of Oregon – Oregon Health Authority (OHA)			Contact Name & Role:	Robert Wood, Information Security Advisor
Project Name:	Integrated Eligibility (IE) System Security Management			Company/Org Name:	State of Oregon – Oregon Health Authority (OHA)
Start Date (MM/DD/YYYY):	8/1/2016	End Date:	12/1/2019	Phone Number:	
Staff Role:	Security Architect	Percentage of Time:	100%	Email:	
Description of relevant experience:	As the Security Architect, Karthik utilized security architecture, compliance and governance skills to lead a team of security engineers to review the security requirements to be met by Client's Integrated Eligibility (IE) system, and planned, designed, implemented and managed the security controls in accordance with CMS MARS-E 2.0 standard and based on integrated control framework for IE security architecture. The experience attained by Karthik includes working with the different teams including development team, technical architects, IT infrastructure team to designing, implementing and managing security controls based on security standards, developing and delivering CMS compliance related documents for the IE System. Karthik is a subject matter specialist in developing compliance deliverables such as the Information Security Risk Assessment (ISRA), Privacy Impact Assessment (PIA), System Security Plan (SSP), POAM and Self-Attestation (SA); periodically assessing security controls for compliance with required security standards, and leading security testers to identify potential security vulnerabilities.				

  

Project #6				Contact	
Company Name:				Contact Name & Role:	
Project Name:				Company/Org Name:	
Start Date (MM/DD/YYYY):		End Date:		Phone Number:	
Staff Role:		Percentage of Time:		Email:	
Description of relevant experience:					

**PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE**

Contractor -	Deloitte Consulting LLP		Candidate Name - Karthik Krishnamurthy		
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 - BenefitsCal Maintenance	1/6/2022	7/30/2024	50%	30.8	15.4
Security Engineering Improvements	1/6/2022	7/30/2024	50%	30.8	15.4
CalSAWS - BenefitsCal Implementation	8/6/2020	1/5/2022	100%	17.0	17.0
Federal Draw Reporting (FDR) Solution	12/2/2019	8/5/2020	100%	8.1	8.1
			0%	0.0	0.0
			0%	0.0	0.0
Totals				86.7	55.9

**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:	California Statewide Automated Welfare System (CalSAWS)			Contact Name & Role:	Joseph Nelson, Chief Privacy Officer	
Project Name:	CalSAWS - BenefitsCal Maintenance and Enhancement (M&E)			Company/Org Name:	CalSAWS Consortium	
Start Date (MM/DD/YYYY):	1/6/2022	End Date (MM/DD/YYYY):	7/30/2024	Phone Number:	[REDACTED]	
Staff Role:	Security Lead and Architect	Percentage of Time:	50%	Email:	[REDACTED]	
Description of relevant experience	As the Security Lead and Architect, Karthik led and managed all the security aspects of BenefitsCal system development, implementation, monitoring, and operational improvements on a cloud-based AWS platform. His responsibilities included review and monitoring of application and AWS cloud infrastructure security controls in compliance with NIST 800-53, and CalSAWS security standards. Throughout the project, Karthik worked with application development teams, technology architects, Consortium Security and vendor teams to implement and maintain security controls based on the BenefitsCal security architecture.					
Project #2				Contact		
Company Name:	Department of Health Care Services (DHCS)			Contact Name & Role:	Chris Bailey, Chief Information Security Officer	
Project Name:	Security Engineering Improvements			Company/Org Name:	DHCS	
Start Date:	1/6/2022	End Date:	7/30/2024	Phone Number:	[REDACTED]	
Staff Role:	Security Project Manager and Architect	Percentage of Time:	50%	Email:	[REDACTED]	
Description of relevant experience	Karthik works directly with the DHCS CISO, security architects, development team, cloud infrastructure team to identify security priorities and initiatives to help the overall program. Karthik leads a team of security engineers to develop, implement, monitor, and improve security capabilities and controls to meet the NIST 800-53 Rev 5 standard. The security projects that are delivered to the client include: define and implement Data Loss Prevention (DLP) capabilities, AWS cloud infrastructure security controls, ransomware preparedness assessment, ServiceNow implementation of Continuous Authorization Module (CAM) with the objective to develop and maintain SSPs, POAMs, migration and integration of custom applications with Azure Entra ID for authentication and Multi-Factor Authentication (MFA) enablement, security architecture design based on integrated control framework, network security enhancements, GenAI Governance frameworks, security incident response table top exercise, Active Directory improvement initiatives, network security improvements.					



Project #3				Contact	
<b>Company Name:</b>	California Statewide Automated Welfare System (CalSAWS)			<b>Contact Name &amp; Role:</b>	Joseph Nelson, Chief Privacy Officer
<b>Project Name:</b>	CalSAWS - BenefitsCal Implementation			<b>Company/Org Name:</b>	CalSAWS Consortium
<b>Start Date (MM/DD/YYYY):</b>	8/6/2020	<b>End Date:</b>	1/5/2022	<b>Phone Number:</b>	
<b>Staff Role:</b>	Project Manager and Information Security Assessment Lead	<b>Percentage of Time:</b>	100%	<b>Email:</b>	
<b>Description of relevant experience</b>	As the Security Lead and Architect, Karthik led and managed all the security aspects of BenefitsCal system development, implementation, maintenance, and operational improvements on a cloud-based AWS platform. His responsibilities included review and monitoring of application and AWS cloud infrastructure security controls in compliance with NIST 800-53, and CalSAWS security standards. Throughout the project, Karthik worked with application development teams, technology architects, Consortium Security and vendor teams to implement and maintain security controls based on the BenefitsCal security architecture.				

  

Project #4				Contact	
<b>Company Name:</b>	Department of Health Care Services (DHCS)			<b>Contact Name &amp; Role:</b>	Richard Green, Chief, Cybersecurity Risk & Compliance Section
<b>Project Name:</b>	Federal Draw Reporting (FDR) Solution Implementation Project			<b>Company/Org Name:</b>	DHCS
<b>Start Date (MM/DD/YYYY):</b>	12/2/2019	<b>End Date:</b>	8/5/2020	<b>Phone Number:</b>	
<b>Staff Role:</b>	Security Architect	<b>Percentage of Time:</b>	100%	<b>Email:</b>	
<b>Description of relevant experience</b>	As the Security Architect, Karthik led a team responsible for reviewing the requirements, develop, implement, monitor, and improve the security controls based on integrated control framework from applicable security standards. Working with the different teams including development team, technical architects, cloud infrastructure team, DHCS ISO Team for implementation, and performing information security evaluation and compliance of the FDR Solution. Karthik attained the experience of leading the team to design and implement security controls, develop the FDR System Security Plan (SSP) that provides an overview of the security and privacy requirements of the enterprise systems and described the controls in place or planned to improve the protection of information system resources. Karthik also gained experience in conducting periodic security reviews of the FDR Solution with the Department of Health Care Services (DHCS) Information Security Office (ISO) and oversaw the security testing activities and evaluation of compliance of FDR Solution with DHCS Security and Privacy policies, FedRAMP, NIST Special Publication 800-53 (current version), SAM, SIMM, and HIPAA.				

			Contact	
Company Name:			Contact Name & Role:	
Project Name:			Company/Org Name:	
Start Date (MM/DD/YYYY):		End Date:		Phone Number:
Staff Role:		Percentage of Time:		Email:
Description of relevant experience				
Project #6			Contact	
Company Name:			Contact Name & Role:	
Project Name:			Company/Org Name:	
Start Date (MM/DD/YYYY):		End Date:		Phone Number:
Staff Role:		Percentage of Time:		Email:
Description of relevant experience				

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE					
Contractor -	Deloitte Consulting LLP		Candidate Name - Karthik Krishnamurthy		
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 - BenefitsCal Maintenance and Enhancement (M&E)	1/6/2022	7/30/2024	50%	30.8	15.4
Security Engineering Improvements	1/6/2022	7/30/2024	50%	30.8	15.4
CalSAWS - BenefitsCal Implementation	8/6/2020	1/5/2022	100%	17.0	17.0
Federal Draw Reporting (FDR) Sc	12/2/2019	8/5/2020	100%	8.1	8.1
Integrated Eligibility (IE) System S	8/1/2016	12/1/2019	100%	40.0	40.0
			0%	0.0	0.0
Totals				126.7	95.9

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:	California Statewide Automated Welfare System (CalSAWS)			Contact Name & Role:	Joseph Nelson, Chief Privacy Officer
Project Name:	CalSAWS - BenefitsCal Maintenance and Enhancement (M&E)			Company/Org Name:	CalSAWS Consortium
Start Date (MM/DD/YYYY):	1/6/2022	End Date (MM/DD/YYYY):	7/30/2024	Phone Number:	
Staff Role:	Security Lead and Architect	Percentage of Time:	50%	Email:	
Description of relevant experien	As the Security Lead and Architect, Karthik led and managed all the security aspects of BenefitsCal system development, maintenance, and operations on a cloud-based AWS platform. His responsibilities included review and updating the security deliverables BenefitsCal System Security Plan (SSP), BenefitsCal Technical System Design document, BenefitsCal Test Plan, BenefitsCal Maintenance and Operations Plan document applying Information Security principles, methods, and techniques.				
Project #2				Contact	
Company Name:	Department of Health Care Services (DHCS)			Contact Name & Role:	Chris Bailey, Chief Information Security Officer
Project Name:	Security Engineering Improvements			Company/Org Name:	DHCS
Start Date:	1/6/2022	End Date:	7/30/2024	Phone Number:	
Staff Role:	ity Project Manager and Arch	Percentage of Time:	50%	Email:	
Description of relevant experien	As the Security Project Manager and Architect, Karthik led a team of security engineers in the development of security deliverables including security architecture design, enterprise System Security Plan (SSP), POAM based on DHCS Security and Privacy policies, and NIST Special Publication 800-53 (current version) applying the applicable information security principles, methods, and techniques.				

Project #3				Contact	
<b>Company Name:</b>	California Statewide Automated Welfare System (CalSAWS)			<b>Contact Name &amp; Role:</b>	Joseph Nelson, Chief Privacy Officer
<b>Project Name:</b>	CalSAWS - BenefitsCal Implementation			<b>Company/Org Name:</b>	CalSAWS Consortium
<b>Start Date (MM/DD/YYYY):</b>	8/6/2020	<b>End Date:</b>	1/5/2022	<b>Phone Number:</b>	
<b>Staff Role:</b>	Project Manager and Information Security Assessment Lead	<b>Percentage of Time:</b>	100%	<b>Email:</b>	
<b>Description of relevant experience:</b>	As the Security Lead and Architect, Karthik led and managed all the security aspects of BenefitsCal system development, maintenance, and operations on a cloud-based AWS platform. His responsibilities included review and updating the security deliverables BenefitsCal System Security Plan (SSP), BenefitsCal Technical System Design document, BenefitsCal Test Plan, BenefitsCal Maintenance and Operations Plan document applying applicable information security principles, methods, and techniques.				

  

Project #4				Contact	
<b>Company Name:</b>	Department of Health Care Services (DHCS)			<b>Contact Name &amp; Role:</b>	Richard Green, Chief, Cybersecurity Risk & Compliance Section
<b>Project Name:</b>	Federal Draw Reporting (FDR) Solution Implementation Project			<b>Company/Org Name:</b>	DHCS
<b>Start Date (MM/DD/YYYY):</b>	12/2/2019	<b>End Date:</b>	8/5/2020	<b>Phone Number:</b>	
<b>Staff Role:</b>	Security Architect	<b>Percentage of Time:</b>	100%	<b>Email:</b>	
<b>Description of relevant experience:</b>	As the Security Architect, Karthik led a team responsible for the development of security deliverables including FDR Privacy Impact Assessment (PIA), System Security Plan (SSP), POAM based on DHCS Security and Privacy policies, FedRAMP, NIST Special Publication 800-53 (current version), SAM, SIMM, and HIPAA applying the applicable information security principles, methods, and techniques.				

Project #5					Contact	
<b>Company Name:</b>	State of Oregon – Oregon Health Authority (OHA)			<b>Contact Name &amp; Role:</b>	Robert Wood, Information Security Advisor	
<b>Project Name:</b>	Integrated Eligibility (IE) System Security Management			<b>Company/Org Name:</b>	State of Oregon – Oregon Health Authority (OHA)	
<b>Start Date (MM/DD/YYYY):</b>	8/1/2016	<b>End Date:</b>	12/1/2019	<b>Phone Number:</b>	[REDACTED]	
<b>Staff Role:</b>	Security Architect	<b>Percentage of Time:</b>	100%	<b>Email:</b>	[REDACTED]	
<b>Description of relevant experience:</b>	<p>As the Security Architect, Karthik led a security engineering team in developing security compliance deliverables such as the Information Security Risk Assessment (ISRA), Privacy Impact Assessment (PIA), System Security Plan (SSP), POAM and Self-Attestation (SA); periodically assessing security controls for compliance with required security standards, and applying the applicable information security principles, methods, and techniques.</p>					

  

Project #6				Contact	
<b>Company Name:</b>				<b>Contact Name &amp; Role:</b>	
<b>Project Name:</b>				<b>Company/Org Name:</b>	
<b>Start Date (MM/DD/YYYY):</b>		<b>End Date:</b>		<b>Phone Number:</b>	
<b>Staff Role:</b>		<b>Percentage of Time:</b>		<b>Email:</b>	
<b>Description of relevant experience:</b>					

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE					
Contractor -	Deloitte Consulting LLP		Candidate Name -	Karthik Krishnamurthy	
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 - BenefitsCal Maintenance and	1/6/2022	7/30/2024	50%	30.8	15.4
Security Engineering Improvements	1/6/2022	7/30/2024	50%	30.8	15.4
CalSAWS - BenefitsCal Implementation	8/6/2020	1/5/2022	100%	17.0	17.0
Federal Draw Reporting (FDR) Solution Imp	12/2/2019	8/5/2020	100%	8.1	8.1
Integrated Eligibility (IE) System Security M	8/1/2016	12/1/2019	100%	40.0	40.0
			0%	0.0	0.0
Totals				126.7	95.9

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:	California Statewide Automated Welfare System (CalSAWS)			Contact Name & Role:	Joseph Nelson, Chief Privacy Officer
Project Name:	CalSAWS - BenefitsCal Maintenance and Enhancement (M&E)			Company/Org Name:	CalSAWS Consortium
Start Date (MM/DD/YYYY):	1/6/2022	End Date (MM/DD/YYYY):	7/30/2024	Phone Number:	[REDACTED]
Staff Role:	Security Lead and A	Percentage of Time:	50%	Email:	[REDACTED]
Description of relevant experience:	As the Security Lead and Architect, Karthik's responsibilities included assessing BenefitsCal data sensitivity using FIPS 199 security categorizations to identify appropriate security controls to protect Personally Identifiable Information (PII) stored and processed by BenefitsCal. He led and managed all the security aspects of BenefitsCal system development, maintenance, and operations on a cloud-based AWS platform. His responsibilities included review and monitoring of application and AWS cloud infrastructure security controls in compliance with NIST 800-53, and CalSAWS security standards. Throughout the project, Karthik worked with application development teams, technology architects, Consortium Security and vendor teams to implement and maintain security controls based on the BenefitsCal security categorization.				
Project #2				Contact	
Company Name:	Department of Health Care Services (DHCS)			Contact Name & Role:	Chris Bailey, Chief Information Security Officer
Project Name:	Security Engineering Improvements			Company/Org Name:	DHCS
Start Date:	1/6/2022	End Date:	7/30/2024	Phone Number:	[REDACTED]
Staff Role:	ity Project Manager and Arc	Percentage of Time:	50%	Email:	[REDACTED]
Description of relevant experience:	Karthik works directly with the security architects to assess data sensitivity using FIPS 199 security categorizations to identify appropriate security controls to protect Personally Identifiable Information (PII) and Protected Health Information (PHI) stored and processed by custom applications managed by DHCS. Based on the security categorization, the required security controls were selected, designed and implemented.				

Project #3				Contact	
<b>Company Name:</b>	California Statewide Automated Welfare System (CalSAWS)			<b>Contact Name &amp; Role:</b>	Joseph Nelson, Chief Privacy Officer
<b>Project Name:</b>	CalSAWS - BenefitsCal Implementation			<b>Company/Org Name:</b>	CalSAWS Consortium
<b>Start Date (MM/DD/YYYY):</b>	8/6/2020	<b>End Date:</b>	1/5/2022	<b>Phone Number:</b>	
<b>Staff Role:</b>	Project Manager and Information Security Assessment Lead	<b>Percentage of Time:</b>	100%	<b>Email:</b>	
<b>Description of relevant experience:</b>	As the Security Lead and Architect, Karthik's responsibilities included assessing BenefitsCal data sensitivity using FIPS 199 security categorizations to identify appropriate security controls to protect Personally Identifiable Information (PII) stored and processed by BenefitsCal. He led and managed all the security aspects of BenefitsCal system development, maintenance, and operations on a cloud-based AWS platform. His responsibilities included review and monitoring of application and AWS cloud infrastructure security controls in compliance with NIST 800-53, and CalSAWS security standards. Throughout the project, Karthik worked with application development teams, technology architects, Consortium Security and vendor teams to implement and maintain security controls based on the BenefitsCal security categorization.				
Project #4				Contact	
<b>Company Name:</b>	Department of Health Care Services (DHCS)			<b>Contact Name &amp; Role:</b>	Richard Green, Chief, Cybersecurity Risk & Compliance Section
<b>Project Name:</b>	Federal Draw Reporting (FDR) Solution Implementation Project			<b>Company/Org Name:</b>	DHCS
<b>Start Date (MM/DD/YYYY):</b>	12/2/2019	<b>End Date:</b>	8/5/2020	<b>Phone Number:</b>	
<b>Staff Role:</b>	Security Architect	<b>Percentage of Time:</b>	100%	<b>Email:</b>	
<b>Description of relevant experience:</b>	As the Security Architect, Karthik led a team responsible for reviewing the requirements, identifying and implementing the security controls based on FIPS 199 security categorizations to identify appropriate security controls to protect Personally Identifiable Information (PII) stored and processed by FDR solution. Working with the different teams including development team, technical architects, cloud infrastructure team, DHCS ISO Team for implementation, and performing information security evaluation and compliance of the FDR Solution. Karthik attained the experience of leading the team to design and implement security controls, develop the FDR System Security Plan (SSP) that provides an overview of the security and privacy requirements of the enterprise systems and described the controls in place or planned to improve the protection of information system resources. Karthik also gained experience in conducting periodic security reviews of the FDR Solution with the Department of Health Care Services (DHCS) Information Security Office (ISO) and oversaw the security testing activities and evaluation of compliance of FDR Solution with DHCS Security and Privacy policies, FedRAMP, NIST Special Publication 800-53 (current version), SAM, SIMM, and HIPAA.				
Project #5				Contact	
<b>Company Name:</b>	State of Oregon – Oregon Health Authority (OHA)			<b>Contact Name &amp; Role:</b>	Robert Wood, Information Security Advisor
<b>Project Name:</b>	Integrated Eligibility (IE) System Security Management			<b>Company/Org Name:</b>	State of Oregon – Oregon Health Authority (OHA)
<b>Start Date (MM/DD/YYYY):</b>	8/1/2016	<b>End Date:</b>	12/1/2019	<b>Phone Number:</b>	
<b>Staff Role:</b>	Security Architect	<b>Percentage of Time:</b>	100%	<b>Email:</b>	
<b>Description of relevant experience:</b>	As the Security Architect, Karthik utilized security architecture, compliance and governance skills to lead a team of security engineers to review the security requirements to be met by Client's Integrated Eligibility (IE) system, and planned, designed, implemented and managed the security controls in accordance with CMS MARS-E 2.0 standard and based on FIPS 199 security categorizations to identify appropriate security controls to protect Personally Identifiable Information (PII) stored and processed by the IE system.				

Project #6				Contact	
Company Name:				Contact Name & Role:	
Project Name:				Company/Org Name:	
Start Date (MM/DD/YYYY):		End Date:		Phone Number:	
Staff Role:		Percentage of Time:		Email:	
Description of relevant experience:					



PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE					
Contractor -	Deloitte Consulting LLP		Candidate Name -	Karthik Krishnamurthy	
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 - BenefitsCal Maintenance and	1/6/2022	7/30/2024	50%	30.8	15.4
Security Engineering Improvements	1/6/2022	7/30/2024	50%	30.8	15.4
CalSAWS - BenefitsCal Implementation	8/6/2020	1/5/2022	100%	17.0	17.0
Federal Draw Reporting (FDR) Solution Imp	12/2/2019	8/5/2020	100%	8.1	8.1
Integrated Eligibility (IE) System Security M	8/1/2016	12/1/2019	100%	40.0	40.0
			0%	0.0	0.0
Totals				126.7	95.9

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:	California Statewide Automated Welfare System (CalSAWS)			Contact Name & Role:	Joseph Nelson, Chief Privacy Officer
Project Name:	CalSAWS - BenefitsCal Maintenance and Enhancement (M&E)			Company/Org Name:	CalSAWS Consortium
Start Date (MM/DD/YYYY):	1/6/2022	End Date (MM/DD/YYYY):	7/30/2024	Phone Number:	[REDACTED]
Staff Role:	Security Lead and A	Percentage of Time:	50%	Email:	[REDACTED]
Description of relevant experience:	As the Security Lead and Architect, Karthik led and managed all the security aspects of BenefitsCal system development, implementation, monitoring, and operational improvements on a cloud-based AWS platform. His responsibilities included review and monitoring of application and AWS cloud infrastructure security controls in compliance with NIST 800-53, and CalSAWS security standards. Throughout the project, Karthik worked with application development teams, technology architects, Consortium Security and vendor teams to implement and maintain security controls based on the BenefitsCal security architecture.				
Project #2				Contact	
Company Name:	Department of Health Care Services (DHCS)			Contact Name & Role:	Chris Bailey, Chief Information Security Officer
Project Name:	Security Engineering Improvements			Company/Org Name:	DHCS
Start Date:	1/6/2022	End Date:	7/30/2024	Phone Number:	[REDACTED]
Staff Role:	ity Project Manager and Arc	Percentage of Time:	50%	Email:	[REDACTED]
Description of relevant experience:	Karthik works directly with the DHCS CISO, security architects, development team, cloud infrastructure team to identify security priorities and initiatives to help the overall program. Karthik leads a team of security engineers to develop, implement, monitor, and improve security capabilities and controls to meet the NIST 800-53 Rev 5 standard. The security projects that are delivered to the client include: define and implement Data Loss Prevention (DLP) capabilities, AWS cloud infrastructure security controls, ransomware preparedness assessment, ServiceNow implementation of Continuous Authorization Module (CAM) with the objective to develop and maintain SSPs, POAMs, migration and integration of custom applications with Azure Entra ID for authentication and Multi-Factor Authentication (MFA) enablement, security architecture design based on integrated control framework, network security enhancements, GenAI Governance frameworks, security incident response table top exercise, Active Directory improvement initiatives, network security improvements.				

Project #3				Contact	
<b>Company Name:</b>	California Statewide Automated Welfare System (CalSAWS)			<b>Contact Name &amp; Role:</b>	Joseph Nelson, Chief Privacy Officer
<b>Project Name:</b>	CalSAWS - BenefitsCal Implementation			<b>Company/Org Name:</b>	CalSAWS Consortium
<b>Start Date (MM/DD/YYYY):</b>	8/6/2020	<b>End Date:</b>	1/5/2022	<b>Phone Number:</b>	[REDACTED]
<b>Staff Role:</b>	Project Manager and Information Security Assessment Lead	<b>Percentage of Time:</b>	100%	<b>Email:</b>	[REDACTED]
<b>Description of relevant experience:</b>	As the Security Lead and Architect, Karthik led and managed all the security aspects of BenefitsCal system development, implementation, maintenance, and operational improvements on a cloud-based AWS platform. His responsibilities included review and monitoring of application and AWS cloud infrastructure security controls in compliance with NIST 800-53, and CalSAWS security standards. Throughout the project, Karthik worked with application development teams, technology architects, Consortium Security and vendor teams to implement and maintain security controls based on the BenefitsCal security architecture.				
Project #4				Contact	
<b>Company Name:</b>	Department of Health Care Services (DHCS)			<b>Contact Name &amp; Role:</b>	Richard Green, Chief, Cybersecurity Risk & Compliance Section
<b>Project Name:</b>	Federal Draw Reporting (FDR) Solution Implementation Project			<b>Company/Org Name:</b>	DHCS
<b>Start Date (MM/DD/YYYY):</b>	12/2/2019	<b>End Date:</b>	8/5/2020	<b>Phone Number:</b>	[REDACTED]
<b>Staff Role:</b>	Security Architect	<b>Percentage of Time:</b>	100%	<b>Email:</b>	[REDACTED]
<b>Description of relevant experience:</b>	As the Security Architect, Karthik led a team responsible for reviewing the requirements, develop, implement, monitor, and improve the security controls based on integrated control framework from applicable security standards. Working with the different teams including development team, technical architects, cloud infrastructure team, DHCS ISO Team for implementation, and performing information security evaluation and compliance of the FDR Solution. Karthik attained the experience of leading the team to design and implement security controls, develop the FDR System Security Plan (SSP) that provides an overview of the security and privacy requirements of the enterprise systems and described the controls in place or planned to improve the protection of information system resources. Karthik also gained experience in conducting periodic security reviews of the FDR Solution with the Department of Health Care Services (DHCS) Information Security Office (ISO) and oversaw the security testing activities and evaluation of compliance of FDR Solution with DHCS Security and Privacy policies, FedRAMP, NIST Special Publication 800-53 (current version), SAM, SIMM, and HIPAA.				
Project #5				Contact	
<b>Company Name:</b>	State of Oregon – Oregon Health Authority (OHA)			<b>Contact Name &amp; Role:</b>	Robert Wood, Information Security Advisor
<b>Project Name:</b>	Integrated Eligibility (IE) System Security Management			<b>Company/Org Name:</b>	State of Oregon – Oregon Health Authority (OHA)
<b>Start Date (MM/DD/YYYY):</b>	8/1/2016	<b>End Date:</b>	12/1/2019	<b>Phone Number:</b>	[REDACTED]
<b>Staff Role:</b>	Security Architect	<b>Percentage of Time:</b>	100%	<b>Email:</b>	[REDACTED]
<b>Description of relevant experience:</b>	As the Security Architect, Karthik utilized security architecture, compliance and governance skills to lead a team of security engineers to review the security requirements to be met by Client's Integrated Eligibility (IE) system, and planned, designed, implemented, managed and enhanced the security controls in accordance with CMS MARS-E 2.0 standard which was based on NIST 800-53 Rev 4 standard. The experience attained by Karthik includes working with the different teams including development team, technical architects, IT infrastructure team to designing, implementing and managing security controls based on security standards, developing and delivering CMS compliance related documents for the IE System. Karthik is a subject matter specialist in developing compliance deliverables such as the Information Security Risk Assessment (ISRA), Privacy Impact Assessment (PIA), System Security Plan (SSP), POAM and Self-Attestation (SA); periodically assessing security controls for compliance with required security standards, and leading security testers to identify potential security vulnerabilities.				

Project #6				Contact	
Company Name:				Contact Name & Role:	
Project Name:				Company/Org Name:	
Start Date (MM/DD/YYYY):		End Date:		Phone Number:	
Staff Role:		Percentage of Time:		Email:	
Description of relevant experience:					

PART 2 – SECURITY MANAGER MINIMUM QUALIFICATIONS SUMMARY TABLE				
Contractor -	Deloitte Consulting LLP		Candidate Name - Karthik Krishnamurthy	
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
Certified Information Systems Security Professional (CISSP)	639116	4/1/2024	3/31/2027	

