



August 20, 2018

To Whom It May Concern:

RE: **Sairaja Challagulla**

I hereby certify that **Sairaja Challagulla**, an **AWS Engineer**, has been and is assigned by his employer **Veridic Solutions LLC** to work on a project named **AWS Cloud Foundations at Caterpillar Building AC, Route 29 at Rench Road, Mossville, Illinois, 61552** as part of a contract between my company, **TEKsystems**, and **Caterpillar, Inc.**

This position requires an individual who has a Master's degree in cybersecurity or equivalent experience. Specifically, this individual's responsibilities on this project include:

- Working in AWS platform and its features including IAM, EC2, EFS, VPC, RDS, CloudWatch, CloudTrail, CloudFormation AWS Configuration, Auto Scaling, CloudFront, S3, SNS, Lambda and Route53.
- Implementing a server less architecture using API Gateway, Lambda, and Dynamo db and deploying AWS Lambda code from Amazon S3 buckets. Created a Lambda Deployment function and configured it to receive events from your S3 bucket.
- Monitoring Scout2 Python script populates JavaScript variables displayed in the HTML report. In addition to displaying the AWS configuration, the AWS Scout2 HTML report highlights high-risk areas automatically. Potential findings are highlight with two different colors such as Red: danger and Orange: warning
- Currently, we are using Python 3.6 as a scripting language by Calling API Boto3 and AWS Lambda. We will be adding the events that are required for execution there by logs will be checked in either Cloud Trail and Cloud Watch
- Responsible for creating and configuring the Amazon Elastic File System (EFS) which provides simple, scalable file storage for use with Amazon EC2 in the

AWS Cloud. Amazon EFS is easy to use and offers a simple interface that allows you to create and configure file systems quickly and easily. With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as you add and remove files, so your applications have the storage when they need it.

- Responsible for calling AWS API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. API that acts as a “front door” for applications to access data, business logic, or functionality from your back-end services, such as workloads running on EC2, code running on AWS Lambda, or any Web application. API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management.
- Monitoring such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise using Guard Duty to detect potentially compromised instances or reconnaissance by attackers.
- Responsible for configuring VPC; such as IP address range, create subnets, and configure route tables, network gateways, and security settings. Both public-facing and private subnets can be created to host specific workloads. VPC peering allows you to connect one VPC with another via a direct network route using private IP space. Internet Access is provided through the following mechanisms such as NAT Gateway - outbound only IPv4, Internet Gateway - inbound/outbound IPv4/IPv6 and Egress-only Internet Gateway - Outbound only IPv6
- Responsible for implementing the Lambda to run code without provisioning or managing servers. With Lambda, we can run our code for virtually any type of application or backend service - all with zero administration. Just upload our code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web. Lambda stores code in Amazon S3 and encrypts it at rest.
- Inbound network connections are blocked by AWS Lambda, and for outbound connections only TCP/IP sockets are supported, and ptrace (debugging) system calls are blocked. TCP port 25 traffic is also blocked as an anti-spam measure
- Responsible for triggering SNS, there are two types of clients—publishers and subscribers—also referred to as producers and consumers. Publishers communicate asynchronously with subscribers by producing and sending a message to a topic, which is a logical access point and communication channel. Subscribers (i.e., web servers, email addresses, Amazon SQS queues, AWS Lambda functions) consume or receive the message or notification over one of the supported protocols (i.e., Amazon SQS, HTTP/S, email, SMS, Lambda) when they are subscribed to the topic.
- Responsible for automating the management of IAM Audit, S3 Audit and monitoring of resources for cross-accounts. Here we are using AWS Identity and Access Management (IAM) roles to grant access to resources in other AWS accounts. This

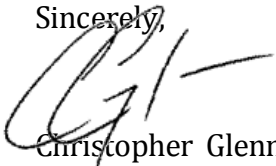
process links API calls that assume a role in one account to resource-related API calls in a different account. When complete, this process will provide a full audit chain from end user to resource access across separate AWS accounts.

This project based work will last through the H-1B period being requested. I have provided redacted versions of the Statement of Work and P.O.'s that Caterpillar has issued to contract with TEKsystems. Caterpillar issues new PO's quarterly or annually, but the project as a whole will continue for several years and we expect Mr. Challagulla to be a part of that project until its conclusion.

Please be advised that Veridic Solutions LLC will retain all rights of control over Mr. Challagulla's work and employment, and that our company has no ability to assign him to any employer.

Should you have any questions please do not hesitate to contact me.

Sincerely,

A handwritten signature in black ink, appearing to be 'CG' followed by a horizontal line.

Christopher Glenn
Delivery Manager

411 Hamilton Blvd, #1610
Peoria, Illinois, 61602
(612) 600-5989