



DevSecOps Engineer

About C2G

C2G delivers technology, cybersecurity, and program management solutions to federal agencies, including the Department of Veterans Affairs. We are seeking a DevSecOps Engineer to support a project with the VA.

Position Summary

The DevSecOps Engineer will support an initiative that connects Salesforce, S-Docs, AWS, and VA Notify to deliver reliable, high-volume outbound Veteran communications — including case correspondence, notifications, and generated documents. The role spans solution assessment, hands-on development, and DevSecOps delivery: evaluating whether the proposed architecture can meet high-volume email and notification requirements, then building, testing, and deploying the integration components that make it work in production.

Key Responsibilities

Solution Assessment & Architecture

- Assess the end-to-end communication workflow across Salesforce, S-Docs, AWS, and VA Notify
- Evaluate S-Docs' ability to generate accurate, consistent HTML/PDF templates, and identify data dependencies, automation triggers, and governance controls needed to maintain template quality at scale.
- Examine AWS Lambda's processing capacity, queueing strategies (e.g., SQS, dead-letter queues), and monitoring capabilities
- Validate the overall solution against operational expectations for scalability, security controls, auditability, observability, and enterprise compliance alignment.
- Document findings, architectural decisions, and identified risks/issues to support traceability and future governance reviews.
- Produce formal solution documentation — data flow diagrams, sequence diagrams, design considerations, and decision logs — to align technical teams, business stakeholders, and support groups.

Development & Integration

- Build and refine Salesforce data models, integration components, error-handling logic, and orchestration needed to support end-to-end processing
- Implement AWS components such as API Gateway endpoints, Lambda functions, SQS queueing, dead-letter queues (DLQs), logging/monitoring pipelines, and services that write delivery results back into Salesforce.
- Automate configuration management, secrets management, and access controls across the integration layer in accordance with federal security baselines and least-privilege principles.
- Integrate application security scanning (SAST/DAST/SCA) into CI/CD pipelines supporting this and other integration workflows.

Required Qualifications

- Bachelor's degree in Computer Science, Information Systems, Cybersecurity, or a related field, or equivalent professional experience.
- Experience in DevOps/DevSecOps or software integration engineering roles, ideally supporting federal government or VA programs.
- Hands-on Salesforce development experience, including Apex, Flow/Process Builder, Lightning Web Components, and REST/SOAP or Bulk API integration patterns.
- Experience with a Salesforce document-generation/templating tool (e.g., S-Docs, Conga, or similar), including HTML/PDF template design, data dependencies, and automation triggers.
- Experience building serverless AWS integrations, including API Gateway, Lambda, SQS/DLQ patterns, and CloudWatch-based monitoring and alerting.
- Experience designing or supporting high-volume, fault-tolerant integration pipelines (e.g., outbound email/notification systems), with attention to throughput, API limits, and latency.
- Practical experience integrating automated security testing (SAST, DAST, SCA) into build and release pipelines.
- Working knowledge of NIST SP 800-53, the Risk Management Framework (RMF), FISMA, and the federal Assessment & Authorization / ATO process.
- Experience with automated testing practices, including high-volume/load testing (50,000+ transactions) and regression test automation.
- Experience deploying through CI/CD pipelines across multiple environments (dev, QA, UAT, production), including tools such as GitLab CI, Jenkins, or Azure DevOps.
- Scripting and automation proficiency in Python, Bash, and/or PowerShell.
- Strong written communication skills, with the ability to produce solution documentation (data flow diagrams, sequence diagrams, decision logs) for both technical and government audiences.
- Must be a U.S. citizen and eligible to obtain and maintain a Public Trust clearance / favorable suitability determination.

Preferred Qualifications

- Direct experience with VA Notify or a similar notification-as-a-service platform (e.g., GOV.UK Notify) for outbound email/SMS delivery and status/bounce reporting.
- Direct experience supporting VA programs, including familiarity with VA Handbook/Directive 6500, the VA Technical Reference Model (TRM), and the VA ProPath SDLC methodology.
- Salesforce certifications (e.g., Platform Developer I/II, Integration Architecture Designer) and/or AWS certifications (e.g., AWS Certified Developer, Solutions Architect).
- Experience with federal GRC/ATO management tools such as eMASS or Xacta.
- Experience with SIEM and log management tools (e.g., Splunk, ELK Stack) supporting continuous monitoring.
- Familiarity with Section 508 accessibility standards and testing tools.
- Experience with container technologies (Docker, Kubernetes/OpenShift) and Infrastructure as Code (Terraform, Ansible, or CloudFormation).
- Experience working within Agile/Scrum delivery teams on federal contracts.

What C2G Offers

- The opportunity to support a mission that directly benefits Veterans and their families.
- A collaborative, security-first engineering culture with investment in automation and modern tooling.
- Competitive compensation and benefits package.
- Professional development support, including certification and training reimbursement.

Additional Information

This position supports a U.S. federal government contract with the Department of Veterans Affairs and is contingent upon successful completion of a government background investigation. C2G is an equal opportunity employer.