AWS re:Inforce

JUNE 10 - 12, 2024 | PHILADELPHIA, PA

GSC221

DoD FedRAMP Equivalency on AWS

Tim J. Sandage

Senior Manager, Security Partners
AWS

Global Security & Compliance Acceleration (GSCA) Program

Global AWS Partner program focusing on accelerating and automating compliance for AWS ISV Partners

Financial services
Healthcare
Public sector
Privacy

Abstract

PreVeil First Company to Achieve Department of Defense FedRAMP Moderate Equivalency

In this lightning talk, learn how PreVeil's encrypted email and file sharing products were configured to meet FedRAMP Equivalency controls for Defense Industrial Base (DIB) contractors by SecureIT, an AWS Global Security & Compliance Acceleration (GSCA) Partner and FedRAMP/CMMC 3PAO.

"PreVeil engaged SecureIT early in their pursuit of FedRAMP Moderate Equivalency. As a trusted and experienced 3PAO that understands the FedRAMP baseline requirements, we were able to provide detailed explanations of noted issues which removed ambiguities and allowed PreVeil to better understand what was specifically needed to more quickly achieve a successful outcome." said David Trout, CEO of SecureIT.

https://www.prweb.com/releases/preveil-first-company-to-achieve-department-of-defense-fedramp-moderate-equivalency-302084624.html

GSCA Partners

SecureIT's range of security and compliance advisory services supports companies at all stages in their AWS journeys

Whether you're just beginning to investigate what AWS means to your security and compliance requirements, or you need an experienced compliance expert to perform your security assessment, SecureIT is an AWS Partner that provides practical and flexible expertise

PreVeil's File Sharing and Email platform enables contractors to protect CUI with end-to-end encryption and supports 102 out of 110 NIST 800-171 controls

Contractors can achieve Zero Trust security for CUI and demonstrate substantial compliance with DFARS 7012 and CMMC

Background – FedRAMP Equivalency

The requirement for defense contractors to use FedRAMP equivalent cloud services to store and process Controlled Unclassified Information (CUI) stems from the DFARS 252.204-7012(b)(2(ii)(D) clause, which states:

> "If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline."

Thomson Reuters, "2023 Risk & Compliance Report."

Protecting Controlled Unclassified Information

The NIST 800-171 document is a companion to NIST 800-53 and dictates how contractors and subcontractors of federal agencies should manage Controlled Unclassified Information (CUI). It's also designed specifically for nonfederal information systems and organizations.

The origins of NIST 800-171 come from Executive Order 13556, signed by President Obama in 2010, mandating that all U.S. federal agencies safeguard CUI more stringently.

Over a Decade of Cyber Initiatives

- February 2013: Executive Order 13636: "Improving Critical Infrastructure Cybersecurity"
- November 18, 2013: Final Rule: "Safeguarding Unclassified Controlled Technical Information"
- May 8, 2015: NARA Proposed Rule: "Controlled Unclassified Information"
- June 19, 2015: NIST SP 800-171: (Final)
- August 11, 2015: OMB draft Guidance: "Improving Cybersecurity Protections in Federal Acquisitions"
- August 26, 2015: Interim Rule: DFARS "Network Penetration Reporting and Contracting for Cloud Services"
- October 8, 2015: DoD Class Deviation – Multifactor authentication (local/network access) – 9 mos.
- December 30, 2015: Interim Rule: "Network Penetration …" (defers cyber obligation to 12/31/2017)
- September 14, 2016: NARA Final Rule, "Controlled Unclassified Information"
- June 2019: CMMC (1.0) announced
- February 2020: CMMC (1.0) Model documents
- September 2020: CMMC Interim Final Rule (IFR) Published; Effective Nov. 30, 2020
- November 2021: CMMC 2.0 announced (5 levels compressed to 3; SP 800-171 baseline)
- December 2021: DoD publishes Level 1 and Level 2 Scoping Guidance & Assessment Guides
- March 22, 2023: Final Rule, Use of Supplier Performance Risk System (SPRS) Assessments
- May 3, 2023: Proposed Rule, Expanding Defense Industrial Base (DIB) Cybersecurity (CS) Activities
- May 10, 2023: NIST SP 800-171 Rev. 3 Initial Public Draft
- December 21, 2023: The office of the CIO, US DoD, issued a memo defining the criteria for cloud service providers to be FedRAMP Moderate baseline equivalent

Benefits of using GSCA Program Partners

Deep security and compliance expertise

Expert vetted AWS Partners with diverse technical and industry expertise

Comprehensive compliance solutions via AWS Marketplace

GSCA Program Partners have built pre-vetted solutions to meet compliance goals

Global presence

Partners with regional presence in NAMER, ANZ, APJ, EMEA, and more

How the engagement process works

END-TO-END COMPLIANCE SUPPORT FOR AWS PARTNERS

Initial 30-min intro call

- GSCA Program overview
- Compliance process overview
- Available AWS resources

Connect Partners with GSCA Partners

Connect the ISVs with GSCA Partners that can help with their compliance journey

Ongoing support & engagement

The GSCA team is here to support the ISVs and Partners throughout the compliance lifecycle

GSCA content

Websites

GSCA customer site

GSCA Partner site

GSCA Partner Bundles site

GSCA AWS Marketplace solutions page

Videos

GSCA YouTube channel

GSCA (ATO on AWS) APN TV page

Case studies

Partner case studies

Explore resources from GSCA

Comply with confidence
Connect with the GSCA team

Launch faster
Find GSCA Program Partners for your compliance needs

Streamline compliance
Provision GSCA Partner Bundles on AWS Marketplace

Navigate your compliance responsibilities
Reference the GSCA Customer Compliance Guide for security best practice guidance mapped to various compliance frameworks

aws.amazon.com/partners/programs/gsca/
aws.amazon.com/partners/programs/gsca/bundles/