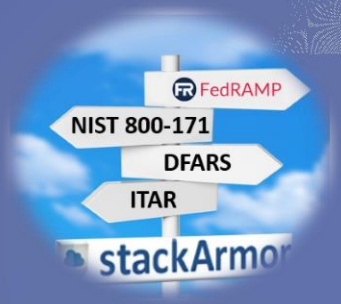
EBOOK



Strategies for meeting DFARS & NIST SP 800-171 requirements with AWS East/West or AWS GovCloud

PUBLISHED BY:

stackArmor

Advanced AWS Partner

www.stackArmor.com

Preface

The United States Department of Defense (DOD) buys over $270 billion worth of products and services from commercial organizations in support of its mission. Thousands of small and large businesses supply a wide variety of products and services from commodities like nails and printers to services such as lawn mowing and complex avionics engineering. Effective Dec 31, 2017 a number of these organizations will need to implement enhanced IT security measures otherwise their ability to do business with the Department of Defense is at risk. Meeting the NIST SP 800-171 compliance requirements can be costly and time consuming. However, DOD has approved a number of certified Cloud Service Providers such as Amazon Web Services (AWS) that are authorized for government use. By leveraging such cloud services, organizations can utilize pre-existing services to meet NIST SP 800-171 security requirements. The table below shows common security requirements and corresponding services.

#	Control Family	AWS Cloud-Native Services
1	Access Control	IAM
2	Awareness and Training	AWS Training Courses on Security, Operations
3	Audit and Accountability	CloudWatch, CloudTrail
4	Configuration Management	Config, Service Catalog, Marketplace
5	Identification and Authentication	Cognito, Directory Service
6	Incident Response	Lambda, SNS, CloudWatch Logs & Metrics
7	Maintenance	Systems Manager, Inspector
8	Media Protection	EBS, S3 Encryption, KMS, Macie
9	Personnel Security	GovCloud: ITAR compliant service by US Persons
10	Physical Protection	AWS FedRAMP ATO
11	Risk Assessment	Trusted Advisor, Artifact
12	Security Assessment	ELK, SplunkCloud
13	System & Communication Protection	WAF, VPC, Security Groups, Sub-nets,
14	System & Information Integrity	Multi-Region, Multi-VPC, Multi-AZ, ASG, ELB

Contents

Chapter 1:

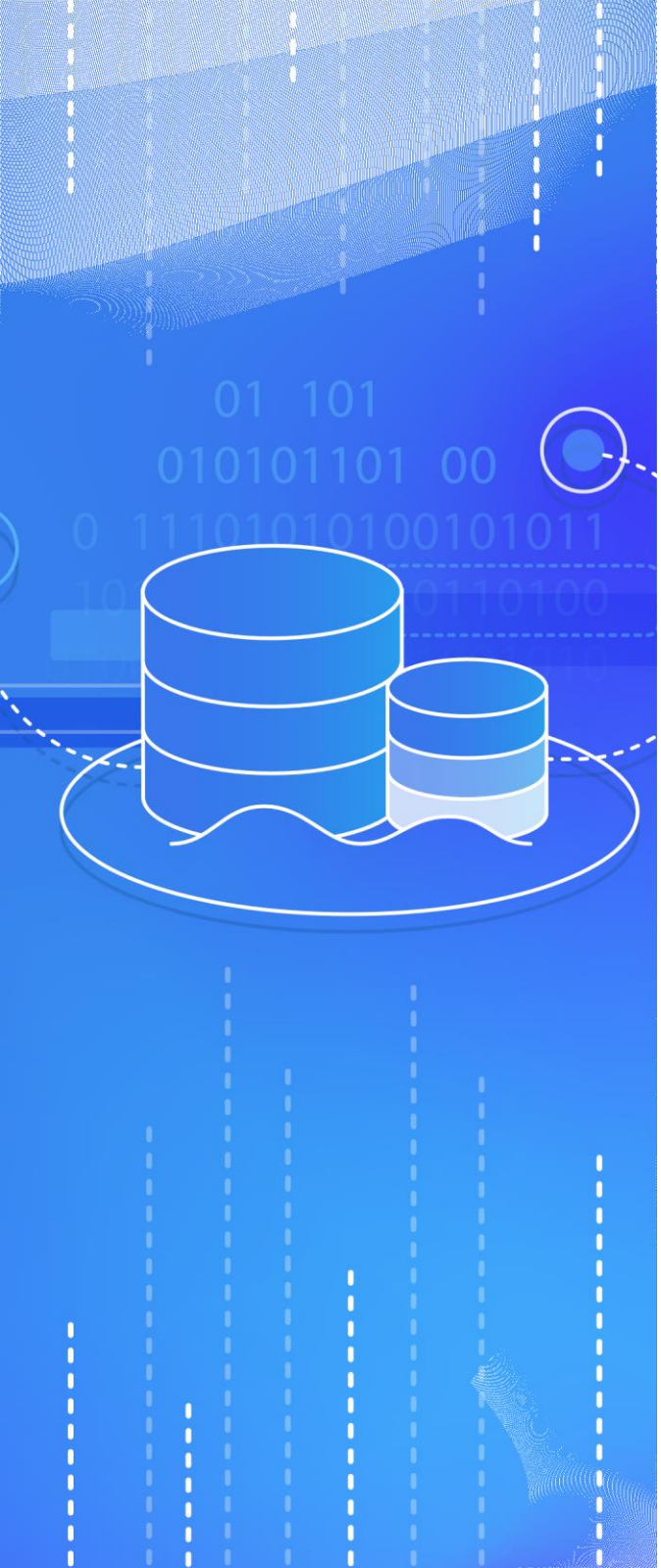
DFARS and NIST SP 800-171

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires organizations doing business with Department of Defense to provide "adequate security" for covered defense information that is processed, stored, or transmitted on their internal information system or network. To provide adequate security, the organization must, at a minimum, implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," not later than December 31, 2017.

Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely. These requirements entail determining what the company policy should be (e.g., what should be the interval between required password changes) and then configuring the IT system to implement the policy. Some requirements will require security-related software (such as anti-virus) or additional hardware (e.g., firewall). NIST SP 800-171 by itself does not provide prescriptive information on how the requirements should be met but additional guidance is provided by looking at relevant security controls that are specified in NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."

Compliance with NIST SP 800-171 is the organization's responsibility through self-attestation that requires demonstrating implementation or planned implementation of the security requirements with a "system security plan" and associated "plans of action." The System Security Plan (SSP) requires developing and documenting system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. The Plans of Action also known as Plan of Actions & Milestones (POAM) to document timelines designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems. Demonstrating compliance with NIST SP 800-171 after December 31, 2017 will require organizations to affirm meeting requirements as covered within their SSP. The SSP may need to be referenced in technical proposals.

> "Federal agencies may consider the contractor's system security plan and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization, and whether or not it is advisable to pursue an agreement or contract with the nonfederal organization."
>
> ***--- NIST SP 800-171***



Chapter 2:

Understanding DFARS & 800-171 Controls

Understand Security Controls and Requirements

800-171 uses the security controls in the moderate baseline of SP 800-53 to tailor controls. The result is 109 security requirements broken up into 14 control families as shown below.

Control Family	Controls	Control Family	Controls
Access Control	22	Media Protection	9
Awareness & Training	3	Personnel Security	2
Audit & Accountability	9	Physical Protection	6
Configuration Management	9	Risk Assessment	3
Identification & Authentication	11	Security Assessment	3
Incident Response	3	System & Communications Protection	16
Maintenance	6	System & Information Integrity	7

Classify Data Sensitivity and Risk Context

Every organization should make an assessment of their risk profile based on the sensitivity of the data. While it is the responsibility of the Government agency to specify CUI, proactive and responsible organizations should be ready with their own assessment. NIST FIPS 199 provides a framework to categorize data and the risk profile based on confidentiality, integrity and availability impact levels. Additionally, organizations should also consider if they have any specific ITAR obligations. This analysis assists with establishing a holistic assessment of the data and risk transiting the environment.

Ensure Flow-downs to Sub-contractors

DFARS 252.204-7012 requires flowing down compliance with NIST SP 800-171 requirements to sub-contractors. Verification of compliance with 800-171 flows to the contracts department of the prime contractor and will require reviewing the SSP and POAM at a minimum.

Chapter 3:

Strategies for meeting DFARS and NIST SP 800-171 requirements

Organizations looking to meet DFARS and NIST SP 800-171 requirements must consider *time to compliance*, financial investment and complexity of the systems involved. Given that the deadline for implementation is December 31, 2017, time to compliance is critical.

Leveraging FedRAMP Accredited Cloud Service Providers

FedRAMP accredited cloud services at the moderate level (based on FIPS 199) or commensurate DOD IL-4 are viable options and allow organizations to inherit and leverage existing controls. Amazon Web Services (AWS) East/West and GovCloud regions are readily available hosting options. The GSA FedRAMP Program Office and DISA have provided the Authority To Operate (ATO) for both AWS East/West and AWS GovCloud regions at the FedRAMP Moderate level. This allows organizations to take advantage of an existing certified infrastructure as a service (IaaS) environment. Organizations have the option to consider AWS East/West or AWS GovCloud – in the event there are ITAR responsibilities then AWS GovCloud should be considered.

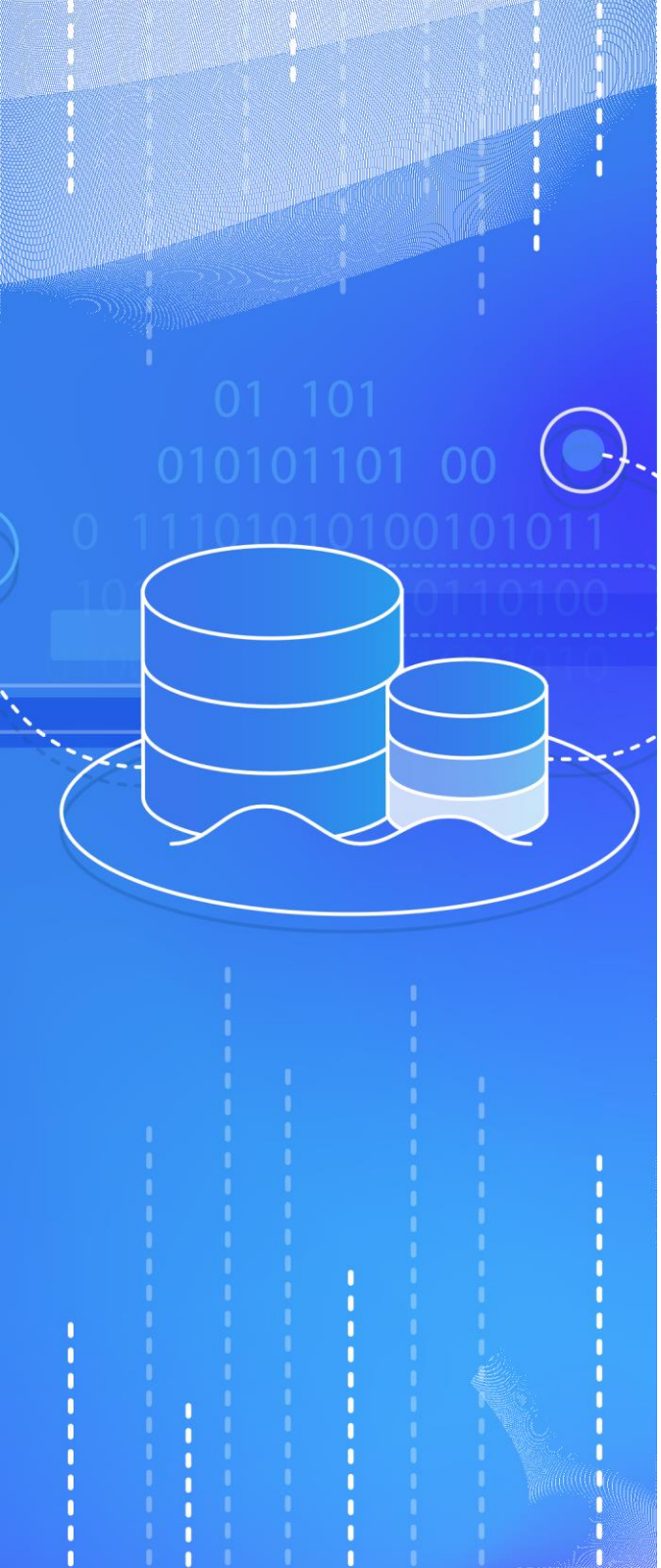
Infrastructure Carve-out for DOD and Government Work

Many organizations are considering creating separate dedicated environments just for government and defense related work. This approach helps reduce the cost and adoption impact especially if DOD or Government work is just a sub segment of the overall business portfolio. There are a number of on-demand services and solutions such as Storage, File Shares, Virtual Desktops and potentially even Email or Portal services for exchanging information.

Outsourcing or Implementing Internally

Creating a compliant solution requires advanced information technology engineering skills that include multiple disciplines. Specific areas of expertise required include infrastructure engineering, networking, security and compliance architecture. A mix-and-match approach that leverages existing capabilities and filling gaps with outsources assistance is a very common way of accelerating the compliance process. Many times engaging outside consulting assistance is required, because internal staff members have “day” jobs and are unable to focus on delivering on extra responsibilities which often leads to delays in implementation.

> “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.
>
> ***--- DFARS 252.204-7012***”



Chapter 4:

Accelerate compliance using AWS Cloud

Using FedRAMP Moderate Accredited Cloud Services

Amazon Web Services (AWS) offers FedRAMP and DOD accredited Infrastructure As-A-Service (IaaS) solutions that are accredited at the Moderate level which make them suitable for NIST SP 800-171. AWS offers two solution options AWS East/West or AWS GovCloud both of which meet Moderate levels controls and are approved by DOD/DISA. The AWS GovCloud Region is an isolated region with ITAR restrictions and also mandates the use of US Persons for support and access to the underlying platform.

Matching Data Classification & Risk to Right AWS Solution

Every organization should make an assessment of their risk profile based on the sensitivity of the data. While it is the responsibility of the Government agency to specify CUI, proactive and responsible organizations should be ready with their own assessment. AWS East/West and AWS GovCloud both are viable options for complying with FedRAMP Moderate controls as required by DFARS. Generally, if the data is seemed highly sensitive and ITAR regulations apply then AWS GovCloud is likely the better option. However, there are cost and capability trade-offs where the AWS GovCloud region is typically 20% more expensive and offers fewer services. Whether to use AWS East/West or AWS GovCloud, is a business decision that every organization must make based on their business, technical and risk parameters.

Define Requirements and Solution Architecture

AWS offers a number of native and value-added services to meet the various information exchange and management use cases. Identifying the services needed such as data or document exchanges can be accomplished using the AWS Data Lake service or Amazon WorkDocs. Information processing can be performed on AWS EC2 virtual instances or virtual desktops (Amazon WorkSpaces). Once the core business services required have been identified and defined, AWS offers a wide variety of logging, monitoring and security management features to meet the various control families specific to NIST SP 800-171.

Chapter 5:

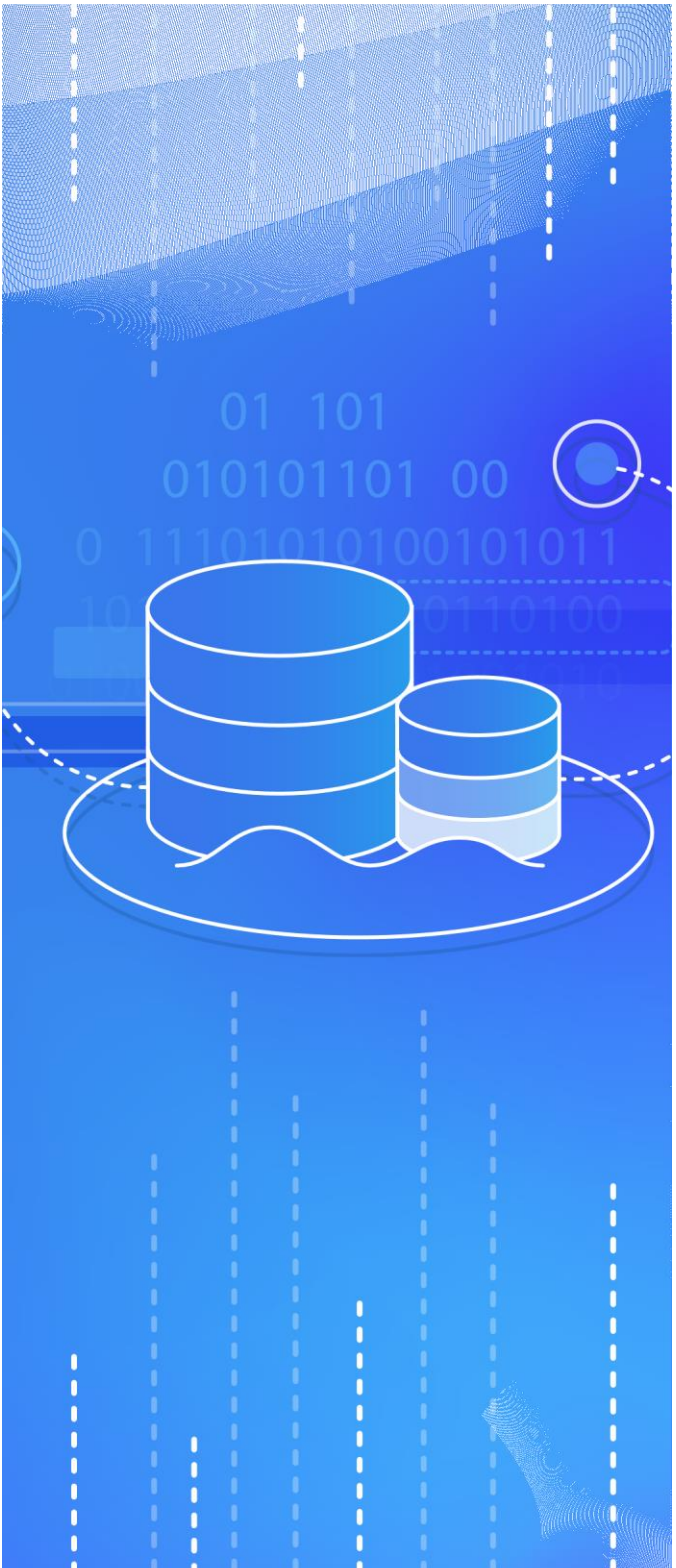
Implementing NIST SP 800-171 Compliant Architecture

Compliance with the DFARS requirement needs the ability to meet the NIST SP 800-171 specified controls that are divided into 14 categories or control families. The table below shows the 14 control families with corresponding AWS cloud native services available to comply with the requirements. The list provided below is just a starting point for ways to meet security requirements.

#	Control Family	AWS Cloud-Native Services
1	Access Control	IAM
2	Awareness and Training	AWS Training Courses on Security, Operations
3	Audit and Accountability	CloudWatch, CloudTrail
4	Configuration Management	Config, Service Catalog, Marketplace
5	Identification and Authentication	Cognito, Directory Service
6	Incident Response	Lambda, SNS, CloudWatch Logs & Metrics
7	Maintenance	Systems Manager, Inspector
8	Media Protection	EBS, S3 Encryption, KMS, Macie
9	Personnel Security	GovCloud: ITAR compliant service by US Persons
10	Physical Protection	AWS FedRAMP ATO
11	Risk Assessment	Trusted Advisor, Artifact
12	Security Assessment	ELK, SplunkCloud
13	System & Communication Protection	WAF, VPC, Security Groups, Sub-nets,
14	System & Information Integrity	Multi-Region, Multi-VPC, Multi-AZ, ASG, ELB

The process of implementing a compliant architecture begins with reviewing FedRAMP approved AWS services. Once the available services are analyzed, the detailed solution architecture blueprint must be created that accommodates the 109 controls required to ensure the solution will meet NIST SP 800-171 requirements. Once the solution is developed, supporting documentation in the form of a System Security Plan (SSP), Plan of Actions & Milestones (POAM) and a IT Contingency Plan (ITCP) should be developed with evidentiary information describing how the controls have been satisfied in the developed solution.

> “
>
> Building a NIST SP 800-171 compliant environment requires following three key steps:
>
> 1. Select FedRAMP Moderate Approved services
> 2. Create solution blueprint that meets the 109 security control requirements.
> 3. Develop supporting SSP, POAM and ITCP.
>
> ”



Chapter 6:

Reducing cost of compliance with AWS, Marketplace and Service Catalog

Amazon Web Services (AWS) offers a rich set of value-added services that reduce the cost of compliance through automation and a self-service marketplace. Government contractors that have distributed locations and diverse services portfolio can maximize operational efficiencies using AWS Marketplace and AWS Service Catalog.

AWS Marketplace

AWS Marketplace is a self-service resource for buying and managing enterprise software that has been vetted and available on a pay-as-you go consumption model. A wide selection of security services such as security incident event management (SIEM), next generation firewalls, hardened AMI's based on Center for Internet Security (CIS) benchmarks and many other categories of ready-made solutions make it easy to deliver compliant services. Software solutions such as SplunkCloud, Palo Alto Networks and many others are readily available with transparent licensing terms friendly for cloud deployments.

AWS Service Catalog

For large Government contractors concerned about ensuring compliance with NIST SP 800-171 and governance, AWS Service Catalog provides the ability to create a shared services delivery model for cost savings across the enterprise. AWS Service Catalog allows the creation of a curated marketplace with authorized products and hardened images that can be shared and federated across teams ensuring that everyone is using authorized components. AWS Service Catalog helps meet Configuration Management related controls.

Conclusion

This eBook is designed US Government and Department of Defense Contractors seeking cost effective and rapid solutions for meeting DFARS and NIST SP 800-171 requirements. The use of FedRAMP Moderate accredited cloud services provides readily consumable solutions for contractors seeking to meet DFARS deadlines for NIST SP 800-171 compliance.

stackArmor

stackArmor is an Advanced AWS certified provider of Security & Compliance, Cloud migration, DevOps enablement, Cloud-native IOT and Data Analytics solutions. As an AWS Authorized Reseller, AWS Public Sector Partner and AWS GovCloud competency holder, stackArmor specializes in delivering secure and compliance oriented IT solutions to regulated industries in Government, Financial Services, Healthcare, Non-profits and Energy. Our experts help protect you from the cyberthreat challenges through systems engineering best practices developed over decades while working with US Federal Agencies requiring compliance with ISO 27001, NIST, FFIEC, FISMA, FedRAMP, DHS and DISA standards.

stackArmor is recognized by Amazon Web Services (AWS) for strong Public Sector and Security competencies and was selected as 1 of 10 inaugural launch partners globally for the AWS Security Competency. Our customers include large public sector and security focused customers in regulated industries with compliance and complex security requirements. We have global delivery model with 24/7 managed services and security support services. Our services on the AWS platform include:

- AWS Solution Architecture and Migration Services
- Cloud Managed Services
- Security Assessment and Authorization Services
- AWS Value-Added Resale (VAR)

Learn more about our services at https://www.stackArmor.com. If you have any questions and want to discuss leveraging AWS for your NIST SP 800-171 compliance requirements please send an email to solutions@stackArmor.com

stackArmor, 1775 Tysons Boulevard, 6th Floor, Tysons VA 22102

aws partner network

Advanced
Consulting Partner

Security Competency
Public Sector Partner
SaaS Partner
GovCloud (US) Service Delivery