NS 18

NIAGARA SUMMIT

CONNECTING
THE WORLD

Federal and DOD Requirements for Niagara

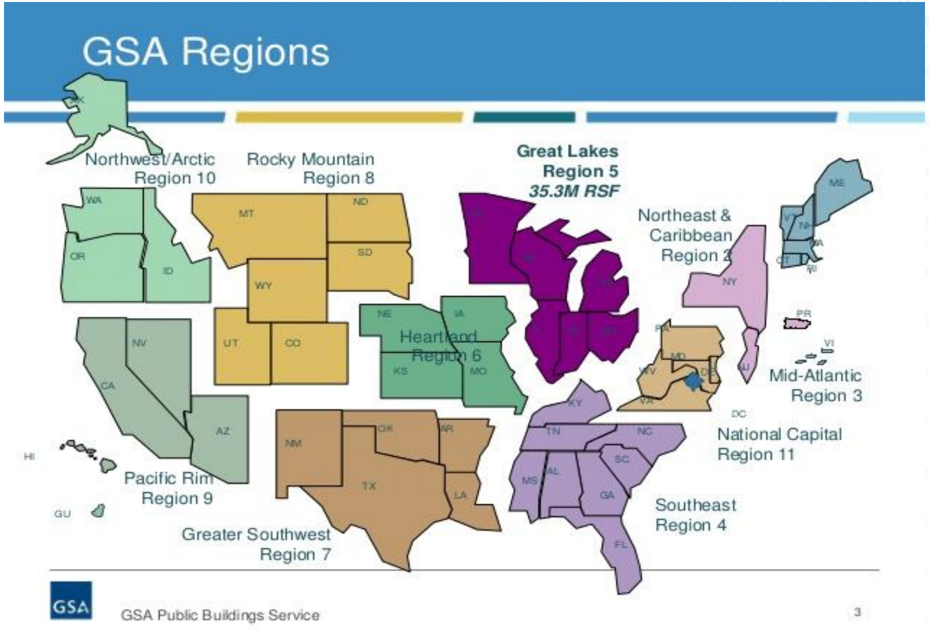
Keith Price - General Services Administration
Jay Kurowsky - Aleta Technologies
Mik Wimbrow - Microsoft Federal

A Perspective from the GSA

Keith Price – General Services Administration.

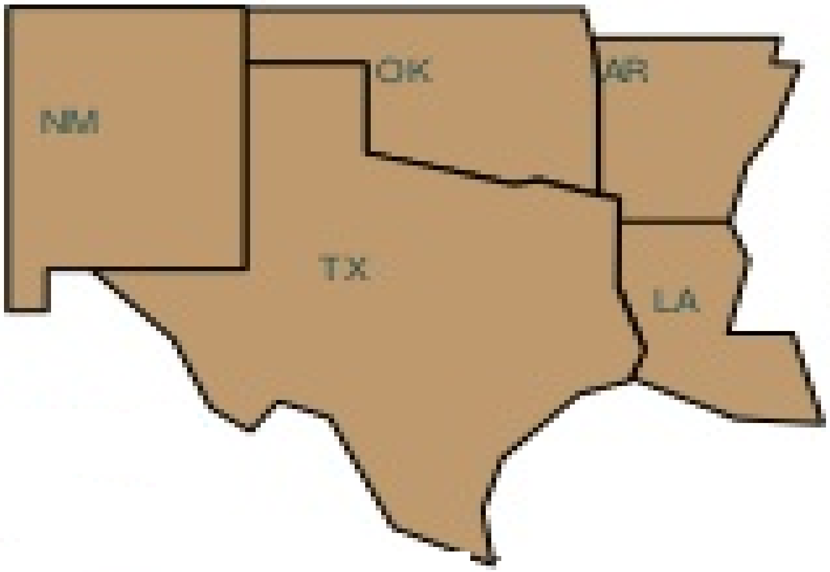
GSA Controls Overview

- GSA manages 377 million square feet of space across almost 10 thousand buildings.
- We have controls equipment in federal space in all 50 states.
- Nine different teams out of Central office in coordination with regional team/SMEs play a role in managing and maintaining all BAS systems.
- We currently utilize over 800 JACEs agency wide.



GSA Controls Cont.

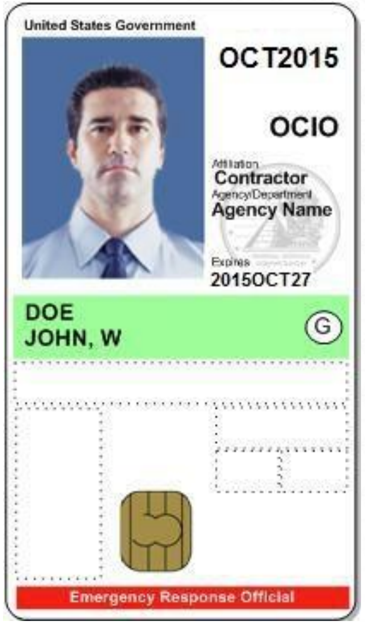
- GSA Region 7 manages roughly 220 JACEs across 100 buildings in 5 states.
- Our team is comprised of five individuals with various controls backgrounds.
- We help manage, troubleshoot, integrate, and analyze control solutions from Fort Worth, Tx.



Working within GSA

Credentials and Access

- Every individual who works in our environment must pass a NACI background check prior to any access.
- PIV card issued provides network and physical access to sites.
- All work done within our buildings must be done on GSA furnished equipment.



United States Government

OCT2015

OCIO

Affiliation
Contractor

Agency/Department
Agency Name

Expires
2015OCT27

DOE
JOHN, W

G

Emergency Response Official

Working with GSA

Communication and Teamwork

- Every aspect of our controls environment is supported or managed by different teams.
- Clear communication and understanding each teams role is ideal.
- Open channels and meetings with Tridium facilitate successful management.

Working with GSA

Vendor Support and Availability

- Most controls contracts solicit open bids and selection based on various criteria.
- Result is a system that incorporates over 50 different vendors.
- We strive to ensure everything remains open!

Working with GSA

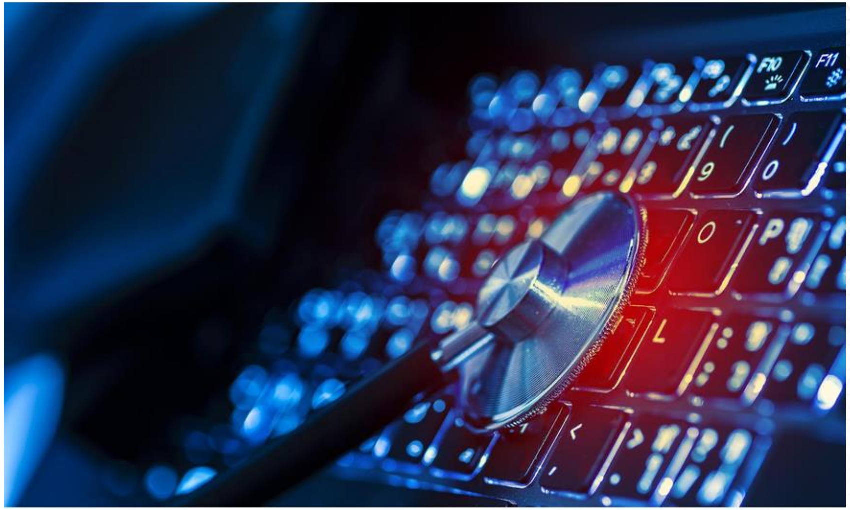
Security

- Expansion of a Building Systems Network (BSN)
- Utilization of FIPS 140-2 compliant standards for transfer of SBU information.
- All hardware and software must undergo scanning for vulnerabilities prior to implementation.

Working with GSA

Security Scanning

- Number one bottleneck in many of our controls projects.
- Vendor support crucial to success
- We have standing meeting with Tridium to address security scan results and seek resolution.



Working with GSA

Asset Management

- New tool to help manage all assets.
- Help facilitate maintenance agreements
- Working with Tridium to improve experience.

niagara
community

Asset Manager

Thanks

Keith Price

General Services Administration

RMF Cybersecurity Process & Insight for DoD Control Systems

Presented by:
Jay Kurowsky
jay.kurowsky@aletatechnologies.com
256-895-8870

Agenda

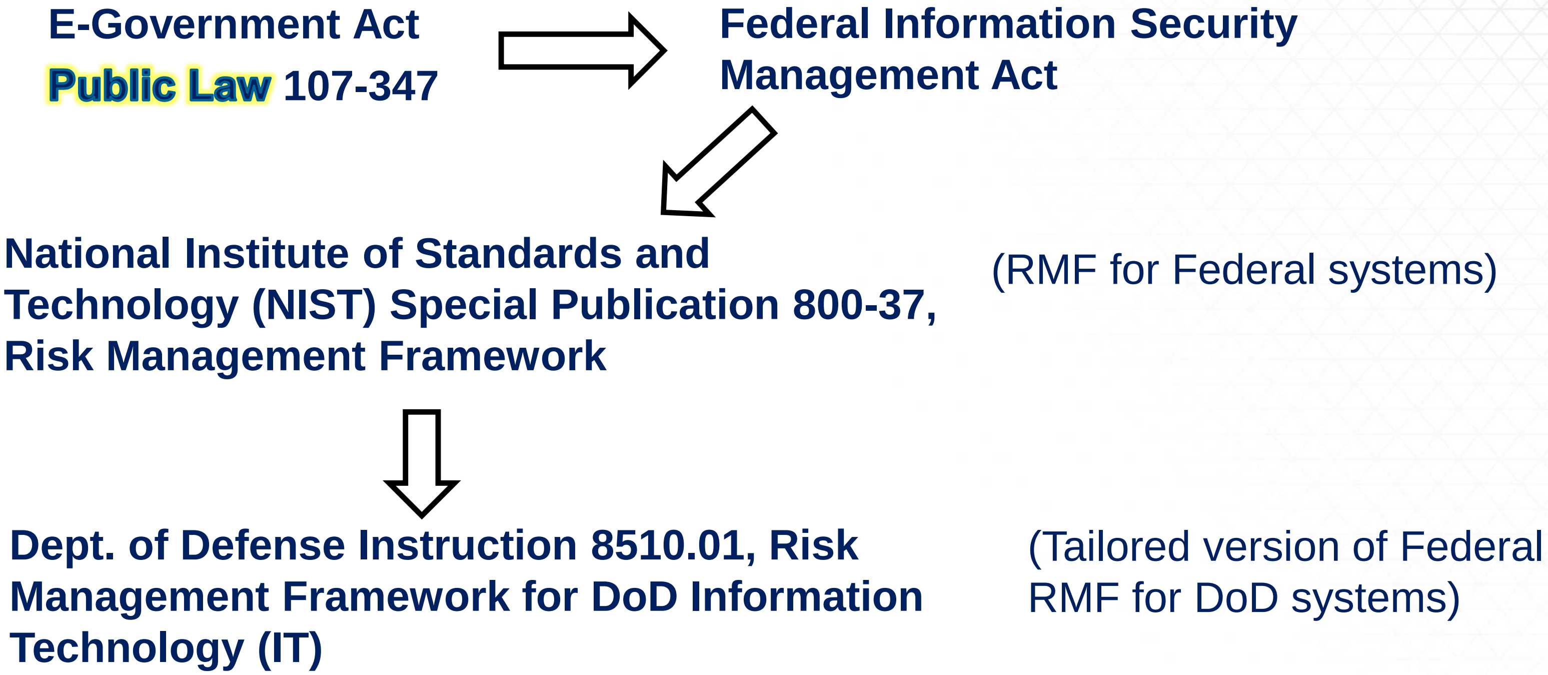
- Risk Management Framework Overview
- RMF Roles and Deliverables
- Questions to Ask
- Subcontractor Cyber Responsibilities
- Security Engineering
- Continuous Monitoring
- FIPS 140-2

So why are we CREDIBLE?

- Experience includes deciding on behalf of the Pentagon what systems were and were not sufficiently secure to connect to Army networks, and advising many dozens of Generals on whether systems were sufficiently secure for operation.

- We have supported over 1,000 systems through RMF and prior processes. We write DoD cybersecurity policy for RMF, and the Office of the Secretary of Defense counts on us to advise them on cybersecurity for control systems.

RMF Pedigree



E-Government Act
Public Law 107-347

Federal Information Security Management Act

National Institute of Standards and Technology (NIST) Special Publication 800-37, Risk Management Framework

(RMF for Federal systems)

Dept. of Defense Instruction 8510.01, Risk Management Framework for DoD Information Technology (IT)

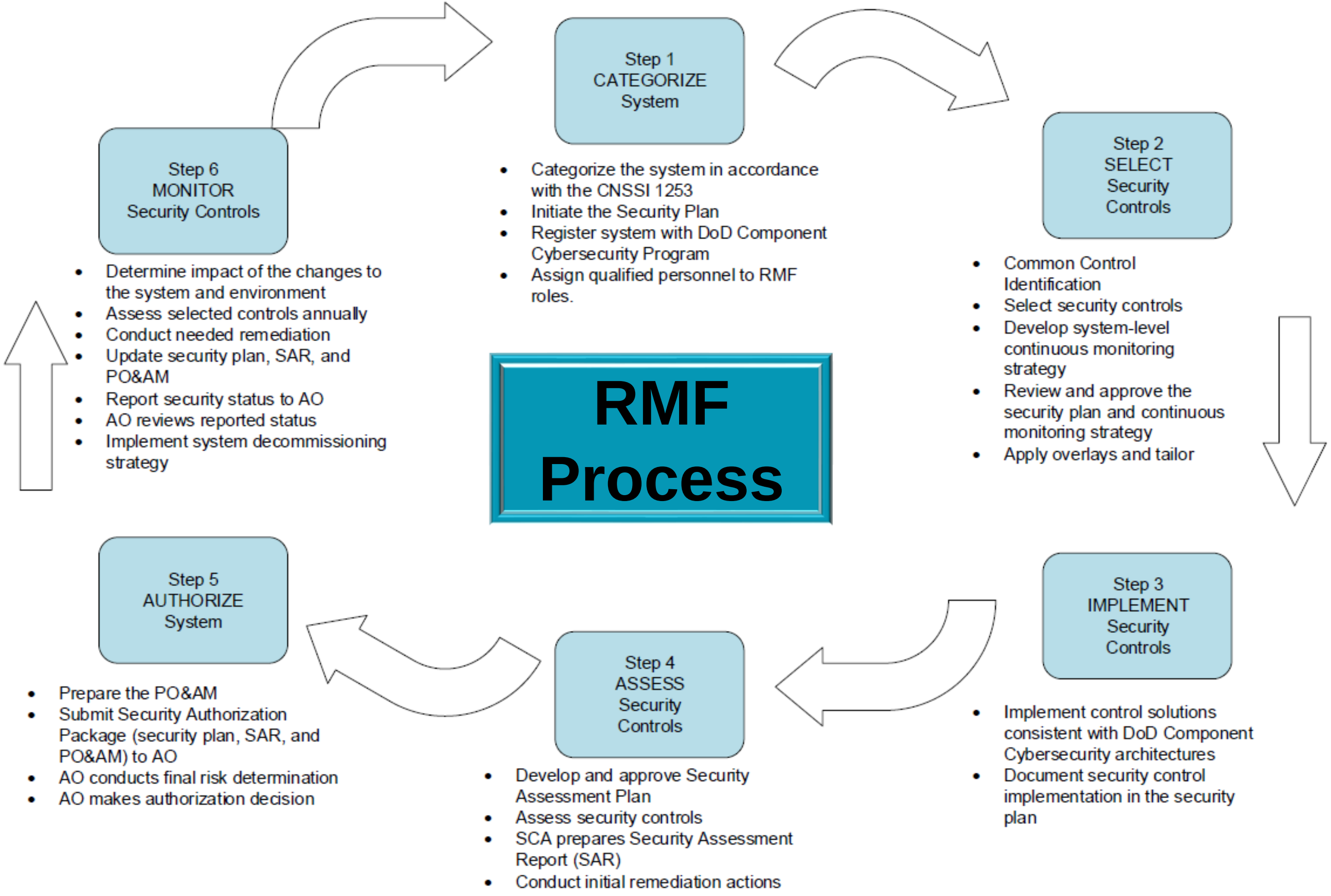
(Tailored version of Federal RMF for DoD systems)

Security Authorization

- The Risk Management Framework (RMF) for DoD Information Technology (IT) is based on National Institute for Standards and Technology (NIST) process
- Per NIST SP 800-37: “Security authorization is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.”
- Per DoD Instruction 8510.01 (“the RMF”): “This instruction applies to:... All DoD IT that receive, process, store, display, or transmit DoD information. These technologies are broadly grouped as DoD IS, platform IT (PIT), IT services, and IT products.”

Note: Control systems are typically PIT

NO AUTHORIZATION =
NO SYSTEM OPERATION



RMF Process

Step 1
CATEGORIZE
System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles.

Step 2
SELECT
Security
Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the security plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3
IMPLEMENT
Security
Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in the security plan

Step 4
ASSESS
Security
Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5
AUTHORIZE
System

- Prepare the PO&AM
- Submit Security Authorization Package (security plan, SAR, and PO&AM) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6
MONITOR
Security Controls

- Determine impact of the changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR, and PO&AM
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

RMF Key Roles

- Authorizing Official (AO): General Officer or civilian equivalent who decides if a system is sufficiently secure to operate and accepts risk for its operation

- Security Control Assessor-Validator: For Army, one of ~12 government officials vetted by Army Headquarters and hired and paid for by System Owner/proponent (other services have differing approaches)

- **System Owner**: Civilian/Military individual with overall responsibility for system implementation and security – can be very problematic for control systems

- Information System Security Officer: The individual responsible for system security, can be contractor, must meet 8570.01M cert requirements

- System Administrator: Generally requires Elevated Privileges, and must meet DoD 8570.01M certification requirements

RMF Deliverables

- CIA AO Concurrence Memorandum
- System Architecture
- Network Topology
- Data Flow Boundary
- Hardware/Software List
- PPS List
- Security Plan
- Continuous Monitoring Strategy
- Risk Assessment
- Completed STIG Checklists/ SCAP Scans

Beware of APMS / DITPR !

- Privacy Impact Assessment
- System Interconnection Agreements
- Configuration Management Plan
- Disaster Recovery Plan/COOP
- Incident Response Plan
- IAVM / Patch Management Plan
- Physical Security Plan
- System Configuration Guide
- System Restoration Checklist
- POA&M

CIA = Confidentiality, Integrity, and Availability
PPS = Ports, Protocols, and Services
STIG = Security Technical Implementation Guide
SCAP = Security Content Automation Protocol

COOP = Continuity of Operations Plan
IAVM = Information Assurance Vulnerability Management
POAM = Plan of Action and Milestones

Questions to Ask

- Will the proposed system be configured as a Standalone/Closed Restricted Network or will it be connected to the COINE, NIPR, DREN or other DISN/DoDIN/GIG network? Or commercial network?

- If the proposed system is connected to an external network, has the external parent network gone thru the RMF process and received an ATO?

- What services will be provided/required by the installation NEC (Active Directory, ACAS scanning, McAfee ePO configuration and updates, SCAP Scans, port scanning, IAVM, etc.) to meet RMF requirements? SLA?

- Is it expected that a contractor will assist the Government customer in the creation of RMF documentation and completion of eMASS tasks such as security control selection, uploading artifacts, and moving the package through the approval chain? How about pre-requisite tasks like DITPR/APMS registration?

NOTE:
eMASS is currently not accessible from dot com!

Questions to Ask, Cont’d

- Will the Government customer require the contractor to perform the system hardening (i.e. STIGs) or will this be handled by a team within the organization like AFCEC, NAVFAC, etc. or by the installation?

- Is remote monitoring and/or maintenance desirable and/or allowable?

- Are there any custom requirements like operational technology (OT) software defined networking (SDN) or other items to augment defense in depth?

- Is there anything else that we should be considering relative to cybersecurity for this ESPC (i.e. new Cyber directives, policies, BBP, TTPs)?

Subcontractor Cyber Tasks

Depending on the Cyber Requirements from the Gov't RFP, the contractor will likely need to perform the following tasks to achieve system ATO:

- ✓ *Perform Security Engineering of Hardware/Software*
- ✓ *Run SCAP and NESSUS scans*
- ✓ *Validate functionality of the system after hardening*

- ✓ *Develop the Security Plan and other RMF deliverables*
- ✓ *Create the Continuous Monitoring Plan*
- ✓ *Work through control inheritance and Service Level Agreements*

- ✓ *Communicate with all cybersecurity and system stakeholders*

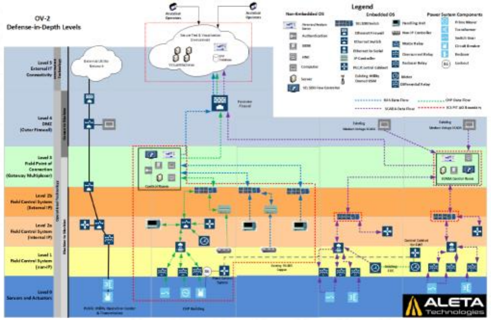
- ✓ *Perform eMASS tasks*

Security Engineering

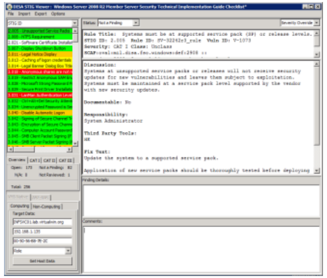
Security Engineering is the RMF phase that requires security architecture design as well as hardening of the hardware and software using Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), STIG Viewer, SCAP Compliance Checker, Nessus vulnerability scans, best practice, and functionality testing.

Deliverables after Security Engineering is complete:

- STIG checklists
- SCAP benchmark scans
- Nessus vulnerability scans
- Application hardening report
- Initial Plan of Actions & Milestones (POA&M)



Security Architecture

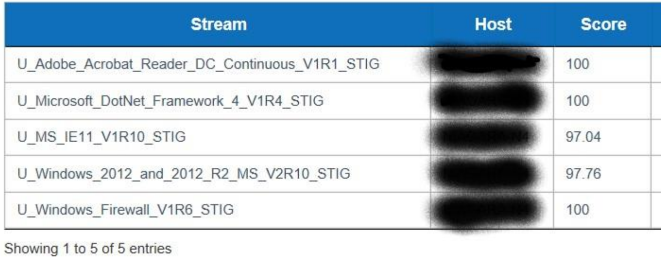


DISA STIG Viewer : Windows Server 2008 R2 Member Server Security Technical Implementation Guide Checklist*

Open: 173 Not a Finding: 82
N/A: 8 Not Reviewed: 1
Total: 256

```
Rule Title:  Systems must be at supported service pack (SP) or release levels.
STIG ID: 2.005  Rule ID: SV-32242r3_rule  Vuln ID: V-1073
Severity: CAT I Class: Unclass
SCAP:oval:mil.disa.fso.windows:def:2908 ::

Discussion:
Systems at unsupported service packs or releases will not receive security
updates for new vulnerabilities and leaves them subject to exploitation.
Systems must be maintained at a service pack level supported by the vendor
with new security updates.

Documentable: No

Responsibility:
System Administrator

Third Party Tools:
HK

Fix Text:
Update the system to a supported service pack.

Application of new service packs should be thoroughly tested before deploying
```

STIG Viewer Tool



Stream	Host	Score
U_Adobe_Acrobat_Reader_DC_Continuous_V1R1_STIG	[redacted]	100
U_Microsoft_DotNet_Framework_4_V1R4_STIG	[redacted]	100
U_MS_IE11_V1R10_STIG	[redacted]	97.04
U_Windows_2012_and_2012_R2_MS_V2R10_STIG	[redacted]	97.76
U_Windows_Firewall_V1R6_STIG	[redacted]	100

Showing 1 to 5 of 5 entries

SCAP Compliance Checker Benchmark Scores

FIPS 140-2

- RMF requires FIPS 140-2 compliant cryptography for Sensitive But Unclassified systems—e.g. controls IA-5(2) and SC-13

- FIPS 140-2 requirements deal with cryptography, not just encryption
  - Identification and Authentication
  - Non-repudiation
  - (and, of course, encryption)

- Niagara 4 has the capability to be compliant if you use it
  - Ensure database compliance
  - Use Public Key Infrastructure via Active Directory

Conclusion

- ✓ Cybersecurity is no longer an afterthought for control system projects
- ✓ Proactive steps have to be taken early, well before construction phase to ensure success.
- ✓ Especially within DoD, without a valid security authorization your system will not be allowed to operate and your project will likely lose money.

Thanks

Jay Kurowsky
jay.kurowsky@aletatechnologies.com
256-895-8870

ALETA
Technologies

www.aletatechnologies.com

Commercial Cloud in the Federal Market

Mik Wimbrow – Microsoft Federal

Let's agree on what “is” and “is not” a Cloud

Optimized
Data Center

Consolidated

Managed

Virtualized

Cost Efficient

+

Cloud Attributes

Pooled
resources

Automation

Self-service

Elasticity

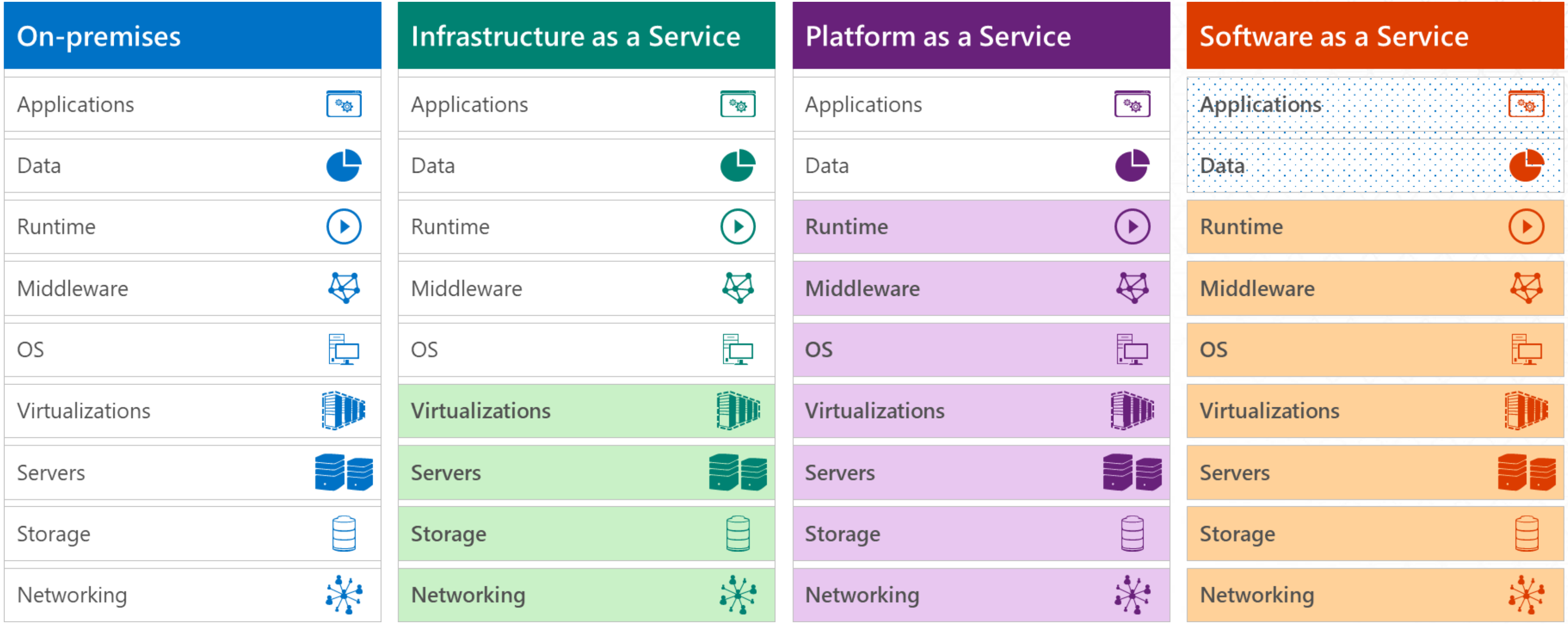
Usage-based

=

Cloud

On Premise: Private Cloud
Off Premise: IaaS, SaaS, PaaS

Cloud Service Type



On-premises	Infrastructure as a Service	Platform as a Service	Software as a Service
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
OS	OS	OS	OS
Virtualizations	Virtualizations	Virtualizations	Virtualizations
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Commercial Cloud in the Federal Market

The Security Continuum

The reason to not to go to the cloud will soon be the reason to go.

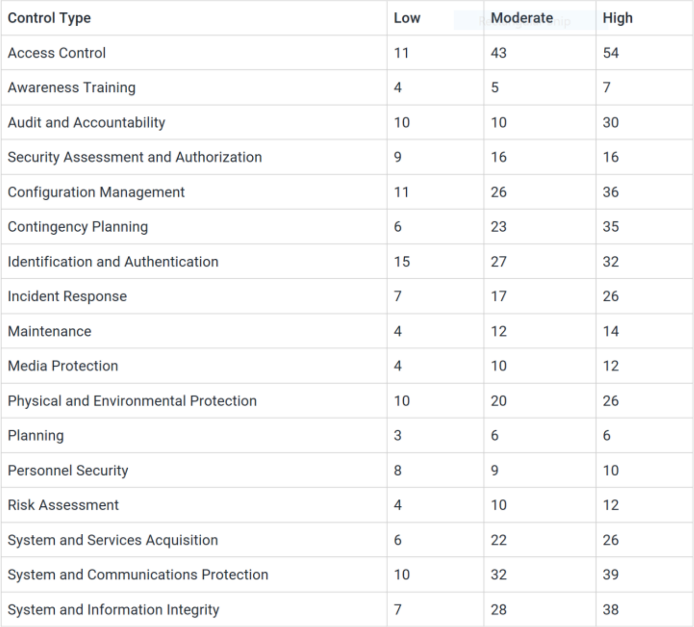
Commercial Cloud Certification - FedRAMP

FIPS199 Defines 3 Ways of Securing Data according to Confidentiality, Availability, and Integrity.

Low – Limited Effect

Moderate - Moderate

High – Severe Adverse Affect on the Organization



Control Type	Low	Moderate	High
Access Control	11	43	54
Awareness Training	4	5	7
Audit and Accountability	10	10	30
Security Assessment and Authorization	9	16	16
Configuration Management	11	26	36
Contingency Planning	6	23	35
Identification and Authentication	15	27	32
Incident Response	7	17	26
Maintenance	4	12	14
Media Protection	4	10	12
Physical and Environmental Protection	10	20	26
Planning	3	6	6
Personnel Security	8	9	10
Risk Assessment	4	10	12
System and Services Acquisition	6	22	26
System and Communications Protection	10	32	39
System and Information Integrity	7	28	38

Commercial Cloud Certification – DISA SRG

Cloud Computing Security Requirements Guide – Defense Information Systems Agency

4 Levels:

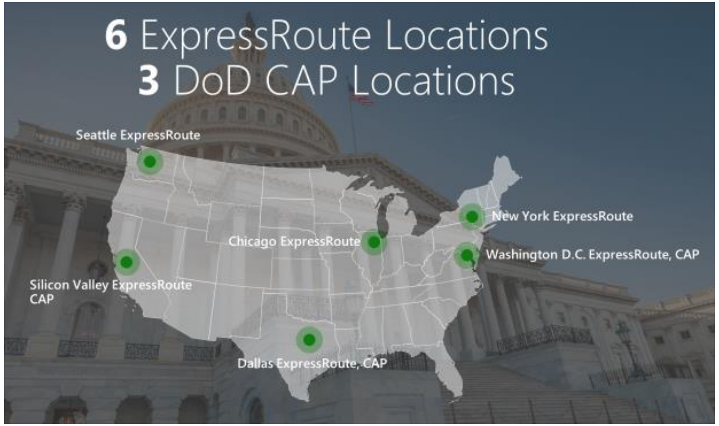
Level 2: Public Release

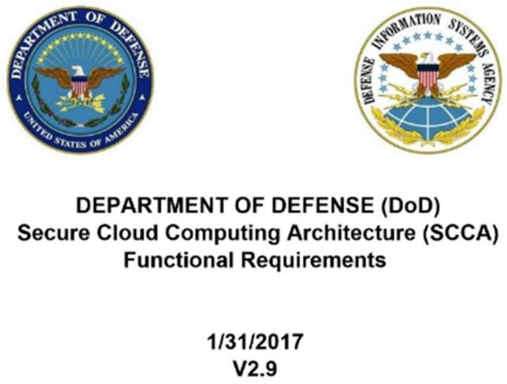
Level 4: Controlled Unclassified Information (CUI)

Level 5: Controlled Unclassified Information – National Security Systems (CUI- NSS)

Level 6: Classified – Secret

Commercial Cloud Connectivity for DoD





DEPARTMENT OF DEFENSE (DoD)
Secure Cloud Computing Architecture (SCCA)
Functional Requirements

1/31/2017
V2.9

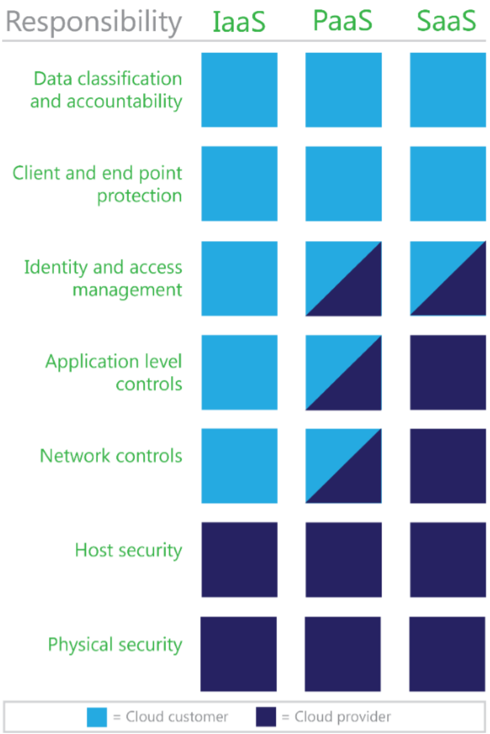
4 Components

CAP – Cloud Access Point (meet me location)
VDSS – Virtual Datacenter Security Stack
VDMS – Virtual Datacenter Management Services
TCCM – Trusted Cloud Credential Manager

Cloud Provider Responsibility for Application Certification

Cloud Security is a Partnership

The more modern an application architecture, the more the CSP is responsible for the controls.



Responsibility	IaaS	PaaS	SaaS
Data classification and accountability	🟦	🟦	🟦
Client and end point protection	🟦	🟦	🟦
Identity and access management	🟦	◪	◪
Application level controls	🟦	◪	⬛
Network controls	🟦	◪	⬛
Host security	⬛	⬛	⬛
Physical security	⬛	⬛	⬛

🟦 = Cloud customer ⬛ = Cloud provider

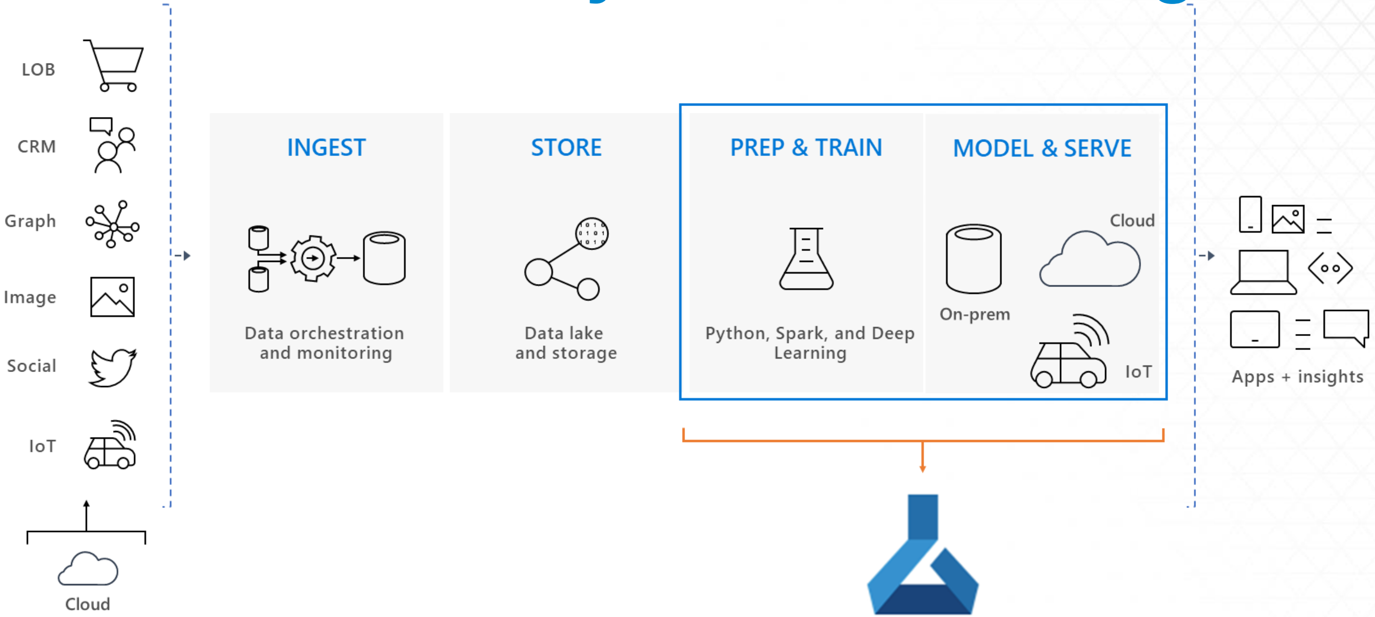
Microsoft Azure Government

Compliant Cloud Solutions for the Federal Government and DoD

- FedRAMP Moderate JAB ATO
- FedRAMP High JAB ATO
- DoD SRG L2 Provisional Authorization
- DoD SRG L4 & L5 Provisional Authorization
- ITAR support
- Dedicated Regions for DoD customers
- Azure Secret - L6 Announcement CY18

- Hyper-scale IaaS and PaaS cloud platform
- Redundant regions to support high availability and disaster recovery scenarios
- Isolation, compliance and connectivity built on Azure Government
- Physical separation through Dedicated infrastructure for compute and storage of DoD workloads
- Express Route connectivity for between Azure Government and O365 Services and DoD customers
- Connectivity through multiple DoD Cloud Access Points and support for disconnected scenarios

AI Dev Platform for Systems of intelligence



Prebuilt: Cognitive Services
Custom: Azure Machine Learning

References

Microsoft Trust Center

www.Microsoft.com/TrustCenter

Azure Blueprint

https://aka.ms/azureblueprint

Thanks

Mik Wimbrow

Microsoft Federal

Federal and DOD Requirements for Niagara

QUESTIONS?

Keith Price - General Services Administration
Jay Kurowsky - Aleta Technologies
Mik Wimbrow - Microsoft Federal