Why FedRAMP and Cloud Security are Crucial to Defense Contractors

June 25, 2019

NeoSystems®
Grow Ahead... We've Got Your Back Office.®

Ed Bassett

Chief Information Security Officer

NeoSystems LLC

Agenda

- Cloud transformation
- Understanding Government security expectations - How the FedRAMP program applies to contractors
- Managing cloud security
- About NeoSystems

“Cloud computing is empowering, as anyone in any part of world with internet connection and a credit card can run and manage applications in the state of the art global datacenters; companies leveraging cloud will be able to innovate cheaper and faster.”

~ Jamal Mazhar, Founder and CEO of Kaavo

WHAT IS “CLOUD”?

Definition can vary by industry or regulation.

As related to Federal Data and Meta-Data…

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
>
> *- NIST SP 800-145*

TL;DR:

> cloud computing … enables network access … to shared computing resources.

WHY ARE CLOUD SERVICES TRANSFORMATIONAL?

- Save money
- Ease of adoption
- Ease of scaling
- Added security capabilities
- Transfer risk (and compliance)
- Improve time to results
- Purchase vendor-driven innovation

FEDERAL ADOPTION

- Federal “Cloud Smart” Strategy adopted in 2018

Cloud Smart focuses on three inter-related areas to drive cloud adoption through building knowledge in government and removing burdensome policy barriers.

Security

Modernize security policies to focus on risk-based decision-making, automation, and moving protections closer to data.

Procurement

Improve the ability of agencies to purchase cloud solutions through repeatable practices and sharing knowledge.

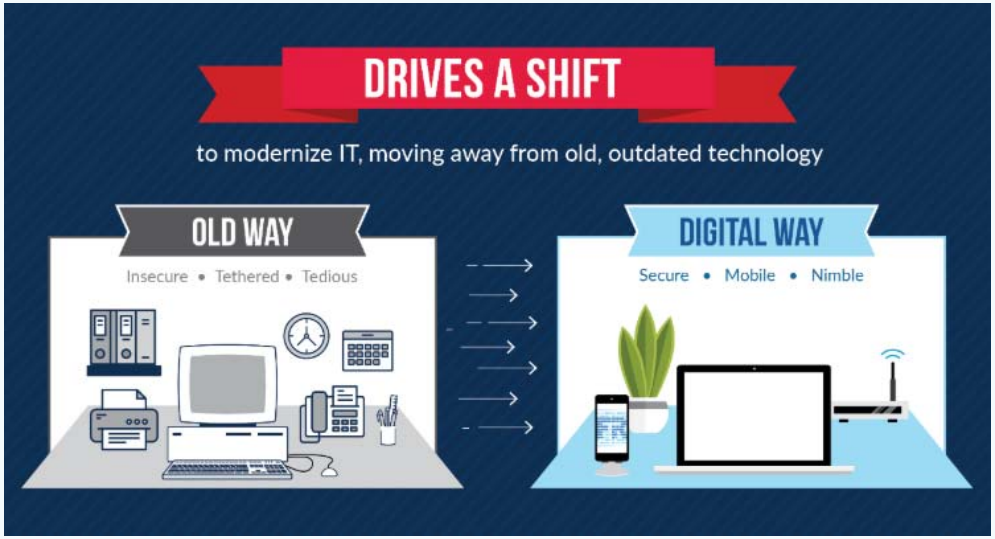
Workforce

Upskill, retrain, and recruit key talent for cybersecurity, acquisition, and cloud engineering.

Source: https://cloud.cio.gov/

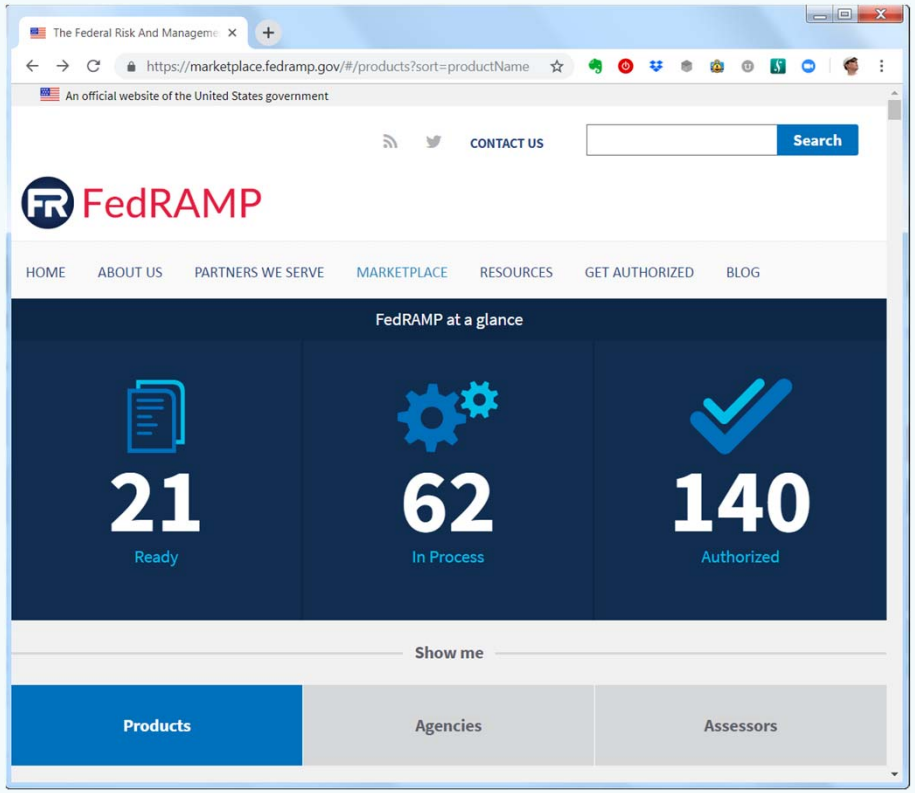
THE FEDRAMP PROGRAM

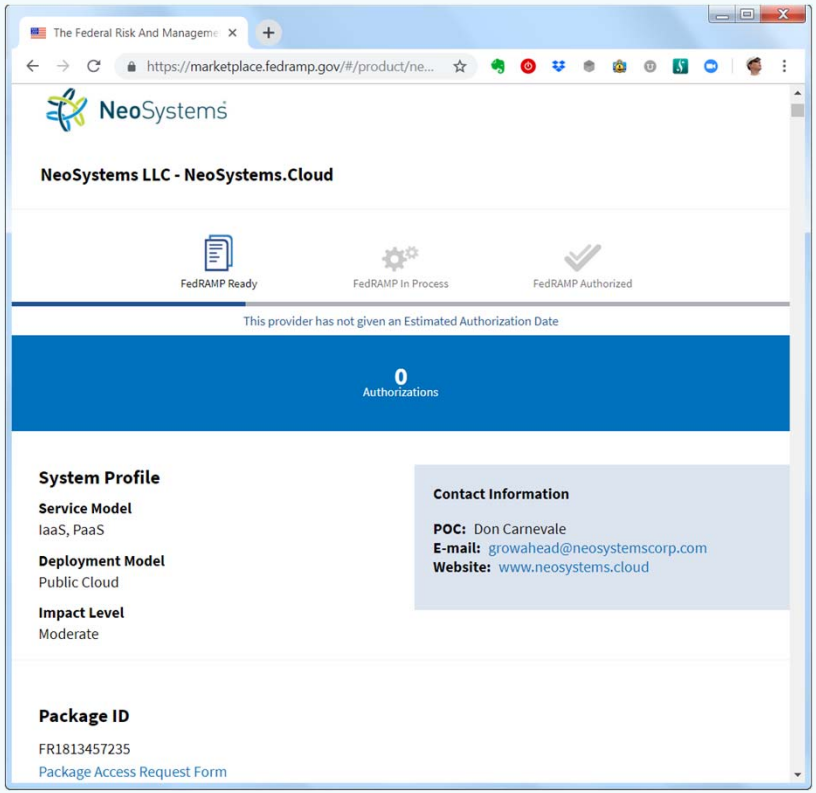
FedRAMP



- Government-wide program established in 2012
- Standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services
- Assess once; re-use across many agencies/use cases
- Mandatory for all agencies and all cloud services

FEDRAMP MARKETPLACE





https://marketplace.fedramp.gov/#/products?sort=productName

HOW DOES THIS APPLY TO GOVERNMENT CONTRACTORS?

FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT

The Federal Information Security Management Act defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

DFARS 252.204-7012

DFARS Safeguarding rules and clauses, for the basic safeguarding of contractor information systems that process, store or transmit Federal contract information. DFARS provides a set of “basic” security controls (SP 800-171) for contractor information systems upon which this information resides.

NIST National Institute of Standards and Technology U.S. Department of Commerce

Tasked by the US Government to develop technology standards, including Information Security standards like SP 800-171, SP 800-53.

CIS Center for Internet Security®

Create publicly-available risk management frameworks, controls, and technical standards cited for use by Federal, State, and Local regulations.

THE DRIVER: DFARS 252.204-7012

(b) Adequate Security (2) (ii) (D)

If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information (CDI) 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 and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

WHY CHOOSE CLOUD HOSTING?

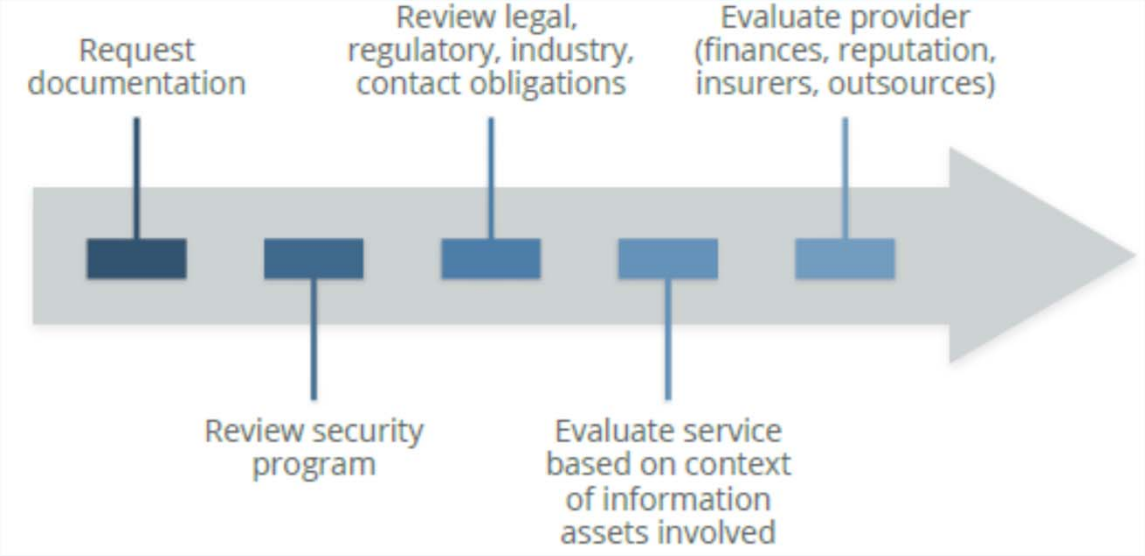
Difficulty Order	Control #	Control Description
1	3.5.3	3.5.3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
2	3.13.11	3.13.11. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
3	3.3.5	3.3.5. Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
4	3.3.6	3.3.6. Provide audit reduction and report generation to support on-demand analysis and reporting.
5	3.7.5	3.7.5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal
6	3.1.19	3.1.19. Encrypt CUI on mobile devices and mobile computing platforms.
7	3.13.13	3.13.13. Control and monitor the use of mobile code.
8	3.3.4	3.3.4. Alert in the event of an audit process failure.
9	3.13.10	3.13.10. Establish and manage cryptographic keys for cryptography employed in organizational systems.
10	3.12.4	3.12.4. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other
11	3.4.8	3.4.8. Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Source: https://my.exostar.com/display/TE/June+2018%3A+Most+Difficult+Controls+in+NIST+800-171

- 1000 suppliers surveyed
- Identified NIST SP 800-171 controls not yet implemented
- Least implemented controls deemed “most difficult”

TOOLS OF CLOUD GOVERNANCE

- Contract – guarantee of service level
- Assessments – customer/self/independent
- Compliance reporting – audit reports, certifications

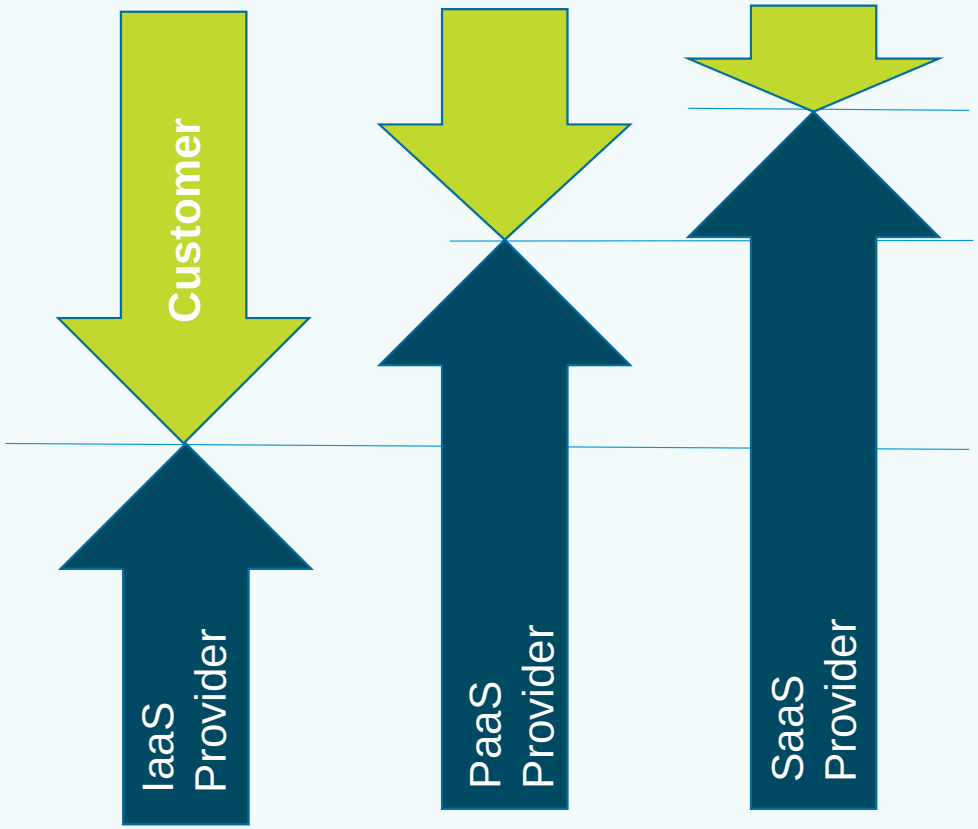


Source: Cloud Security Alliance

SERVICE LEVEL AGREEMENTS

- Cloud computing abstracts the implementation – so instead of hardware and software, you are buying specific performance
- Typical SLAs:
  - Service Availability – Monthly uptime percentage and Recovery Time Objective
  - Data Availability – Recovery Point Objective for Data
  - Response time – Maximum request/response time
- Processing capability and scalability (bandwidth and throughput)
- Geographic / Regional capability
- Personnel Screening (background check, citizenship requirements)

SHARED RESPONSIBILITY



- Data
- Application / DB
- Middleware
- Operating System
- Servers / Virtualization
- Compute, Network, Storage
- Physical Facility

LAYERED SERVICES ON TOP OF CLOUD

- **Cloud providers and third parties offer "managed services" which augment the cloud offering:**
  - Security and compliance
  - Implementation/adoption
  - Monitoring
  - Incident handling
  - Customer service
  - Cost management

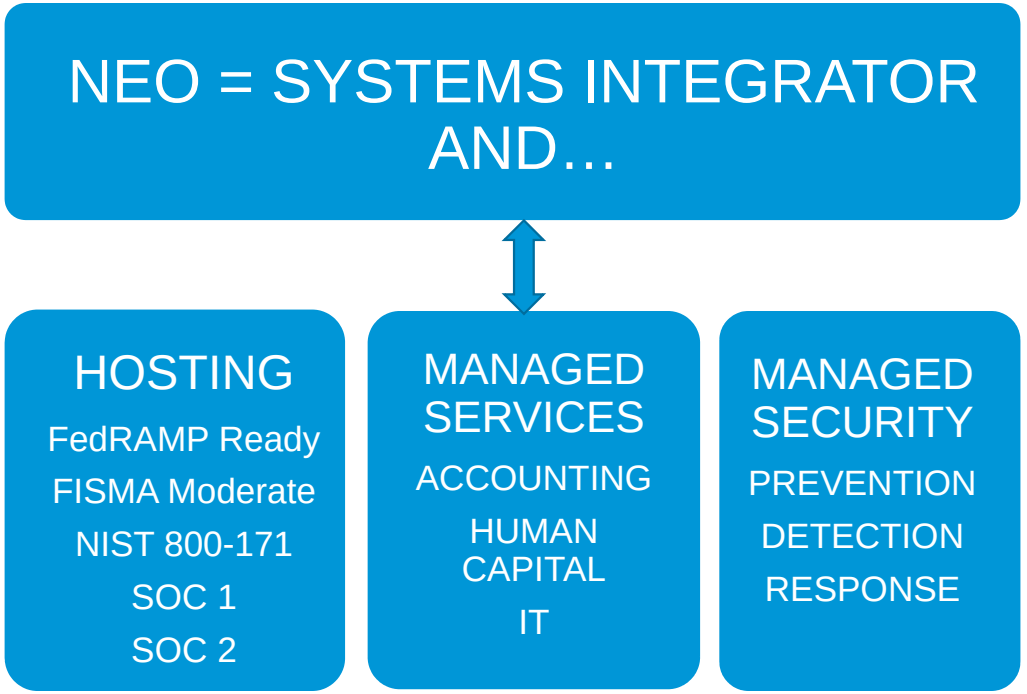
- **Allocate security responsibility:**
  - Cloud service provider
  - Managed service provider
  - Customer

NEOSYSTEMS VALUE PROPOSITION VS DIY

	NeoSystems "CUI Complete" Cloud Hosting	DIY Build using commodity IaaS
Cloud Offering	Managed Service	Infrastructure Only
Staff and Expertise	NeoSystems has dedicated IT staff with expertise in architecting, operating, securing, integrating, upgrading, and maintaining networks, servers, databases, and applications (e.g., Deltek, IBM Cognos), databases, and security.	Company will need to hire staff with expertise deploying Deltek and other applications as well as security, networking, and programming experience.
24/7/365 Monitoring	NeoSystems installs, monitors, validates, and responds to application and infrastructure alerts.	Cloud providers only respond to physical cloud infrastructure alerts. Company will need to install, monitor, validate, and respond to all virtual machine, database, and application alerts.
Compliance and Security **DFARS 7012/NIST 800-171, FedRAMP, SOC 2**	NeoSystems meets Government contracting requirements for the infrastructure and platform as well as application management services.	Cloud provider provides security and compliance for infrastructure only. Company is responsible to ensure that all compliance and security requirements are met.
Disaster Recovery	Application level RTO/RPO defined by SLA and fully managed by NeoSystems.	Company will need to manage and operate to achieve needed RTO/RPO.
Application Patching	Application patching is included in hosting fees. NeoSystems provides the expertise and manages the process.	Company will need to manage the patching and execution of all applications.
O/S Patching	NeoSystems manages the hardening and patching of the operating systems for your application and database servers.	Company will need to harden, patch and maintain the operating systems for application and database servers.
Service Level Agreements	Defined at the application availability level.	Defined at the infrastructure (server) level.
Administrative Control	Defined control processes for system access and changes with client defined POCs and approvers.	Company would need to define and manage the change process.

FINALLY: WHAT WE'RE ALL ABOUT

- Leading provider of Managed Services and Business Management System Implementation & Consulting Services
- Enable, Run & Secure Business Operations
  - Accounting
  - Financial Planning & Analysis
  - Hosting
  - Security
  - IT Infrastructure & Management
  - HR Management
  - Training
- Best-in-Class Technology Partnerships
- Turn Key or Custom Solutions



QUESTIONS?

Thank you!

ed.bassett@neosystemscorp.com

Ed Bassett

Chief Information Security Officer

NeoSystems LLC