Federal CIO Council – Information Security and Identity Management Committee (ISIMC)

Guidelines for the Secure Use of Cloud Computing by Federal Departments and Agencies DRAFT V0.41

Earl Crane, CISSP, CISM
Director, Cybersecurity Strategy
Office of the Chief Information Officer
Department of Homeland Security
ISIMC Cloud Security Working Group Chair

Purpose

- Guidelines provide a risk-based cloud security decision framework
- Assists program managers to select cloud deployment and service models
    - Cloud Deployment and Service Models have varying security characteristics
    - Security Capabilities differ based on characteristics
- Fully supports and coordinates with NIST cloud definition, FedRAMP, and other USG efforts

Deployment Model		Service Model		
		SaaS (Applications)	**PaaS (APIs)**	**IaaS (Virtualization)**
	Public	Use Case 1: Public SaaS	Use Case 2: Public PaaS	Use Case 3: Public IaaS
	Private (Government Dedicated)	Use Case 4: Private SaaS	Use Case 5: Private PaaS	Use Case 6: Private IaaS

FedRAMP/NIST/ISIMC Coordination

	FedRAMP	NIST SP800-53R3	NIST SP800-144	ISIMC
Data Security Impact				
FIPS 199 High Impact		E	I	I
FIPS 199 Moderate Impact	E	E	I	I
FIPS 199 Low Impact	E	E	I	I
Deployment Model				
Public	E	I	E	E
Private		I		E
Service Model				
IaaS	I		E	E
PaaS	I		E	E
SaaS	I		E	E

(E)xplicity or (I)mplicitly addressed

Threat

High Risk Threats

- Well-resourced, highly-motivated groups of cyber-warriors
- Both aggressive and pervasive
- Often referred to as the Advanced Persistent Threat in public media

Medium Risk Threats

- Criminals to steal identity and money
- Varying technical sophistication

Low Risk Threats

- Internet Pollution
- Threats against every user

Sixteen Cloud Security Domains

1. **Architectural Framework for Government Cloud Computing**
2. **Encryption, Key Management, and Media Protection**
3. **Identification, Authentication, and Access Control Management**
4. **Virtualization and Resource Abstraction**
5. **Portability and Interoperability**
6. **Application Security**
7. **Security Risk Assessment, Authorization, and Management**
8. **Privacy, Electronic Discovery, and other Legal Issues**
9. **Contingency Planning**
10. **Data Center Operations, Maintenance, Configuration, Physical, and Personnel Security**
11. **Incident Response**
12. **Compliance, Audit, and Accountability**
13. **Cloud Lifecycle Management**
14. **Awareness and Training**
15. **System and Communication Protection**
16. **System and Information Integrity**

Federal Cloud Security Top 20

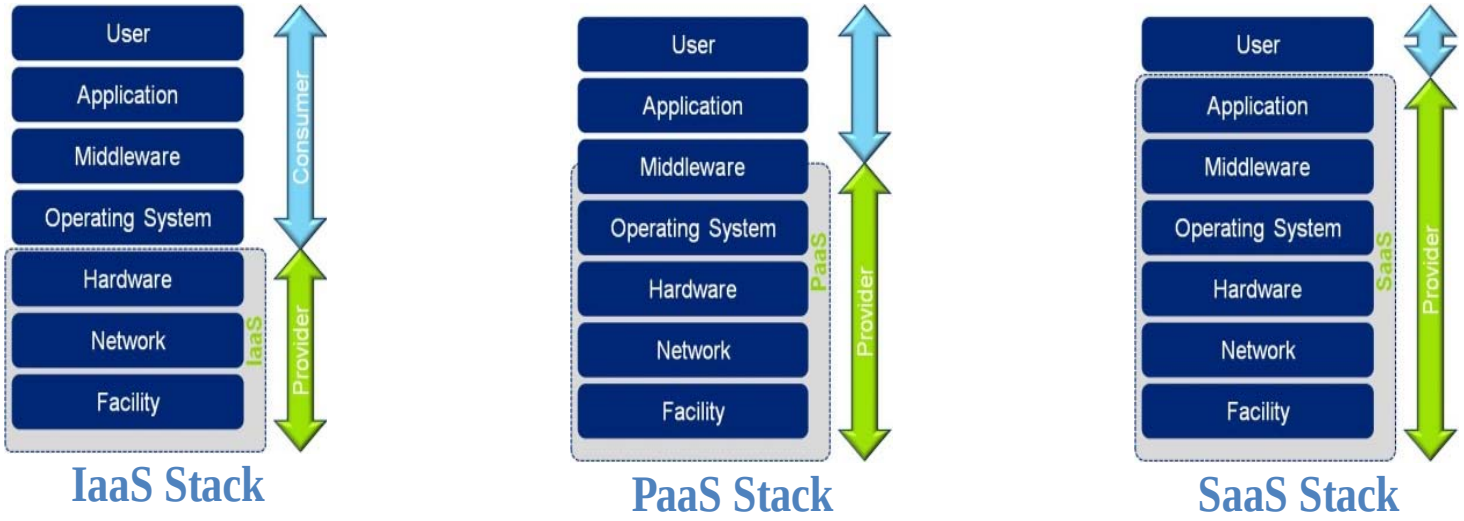
1. Different cloud architectures (SaaS/PaaS/IaaS) have different levels of security visibility and responsibility
2. Data Element Encryption for confidentiality and separation
3. Key management in coordination with Identity, Credentialing, and Access Management (ICAM)
4. Strong authentication, including the use of PIV and PIV-Interoperable
5. Virtualization and resource abstraction. Challenges are specific to the deployed technology, architecture, and Service Models.
6. Cloud portability and interoperability standards.
7. Application security controls including code reviews, vulnerability assessments and independent validation.
8. Utilize the FedRAMP process for risk assessment and authorization for shared resources such as cloud computing.
9. Control data and access for privacy compliance, audit and redress requirements, and breach notification issues.
10. Contingency Planning still required to meet agency requirements
11. Shared capability complicates ownership and governance
12. Government system boundary definitions, compartmentalization, and inventory identification
13. Some government-specific security requirements may not be met today in certain public cloud environments
14. Incident response and computer forensics in a cloud environment require fundamentally different tools, techniques, and training.
15. Accountability can never be outsourced from the Authorizing Official (AO).
16. New opportunities exist for real-time audit capabilities, but requires new continuous monitoring and audit technologies.
17. The System Development Life Cycle (SDLC) in a cloud requires ownership of information throughout the lifecycle.
18. Awareness and Training focusing on risks of information disclosure and data protection.
19. Cloud compartmentalization, isolation, and system boundaries. Use of security services like Trusted Internet Connections (TIC) and DNSSEC.
20. Integrity controls vary by Service Models

Earl.Crane@DHS.gov

Federal Cloud Security Top 20

- #1. Different cloud architectures (SaaS/PaaS/IaaS) have different levels of security visibility and responsibility

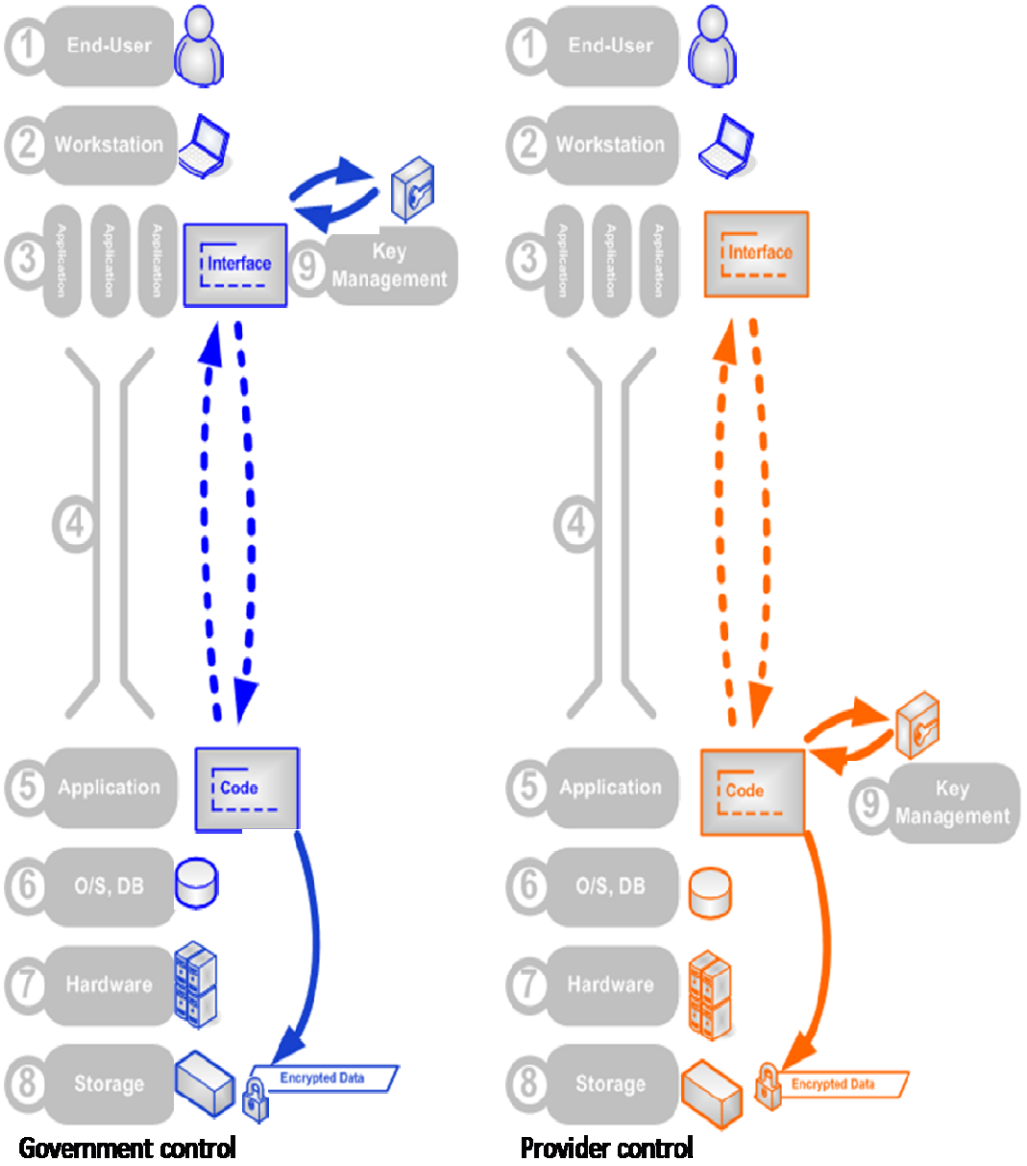
  (Domain 1: Architectural Framework for Government Cloud Computing)



Federal Cloud Security Top 20

- #2. Data Element Encryption for confidentiality and separation
- #3. Key management in coordination with Identity, Credentialing, and Access Management (ICAM)

  (Domain 2: Encryption, Key Management, and Media Protection)



Federal Cloud Security Top 20

- #4. Strong authentication, including the use of PIV and PIV-Interoperable

  (Domain 3: Identification, Authentication, and Access Control Management)

Assurance Level Impact Profiles				
Potential Impact Categories for Authentication Errors	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Federal Cloud Security Top 20

- #5. Virtualization and resource abstraction. Challenges are specific to the deployed technology, architecture, and Service Models.

  (Domain 4: Virtualization and Resource Abstraction)

- #6. Cloud portability and interoperability standards.

  (Domain 5: Portability and Interoperability)

- #7. Application security controls including code reviews, vulnerability assessments and independent validation.

  (Domain 6: Application Security)

Federal Cloud Security Top 20

- #8. Utilize the FedRAMP process for risk assessment and authorization for shared resources such as cloud computing.

  (Domain 7: Security Risk Assessment, Authorization, and Management)

- #9. Control data and access for privacy compliance, audit and redress requirements, and breach notification issues. Review:
  - Terms Of Service (TOS)
  - Cloud provider privacy policies
  - Privacy Impact Assessments (PIA)
  - Fair Information Practice Principles (FIPPs)

  (Domain 8: Privacy, Electronic Discovery, and other Legal Issues)

Federal Cloud Security Top 20

- #10. Contingency Planning still required to meet agency requirements
- #11. Shared capability complicates ownership and governance

(Domain 9: Contingency Planning)

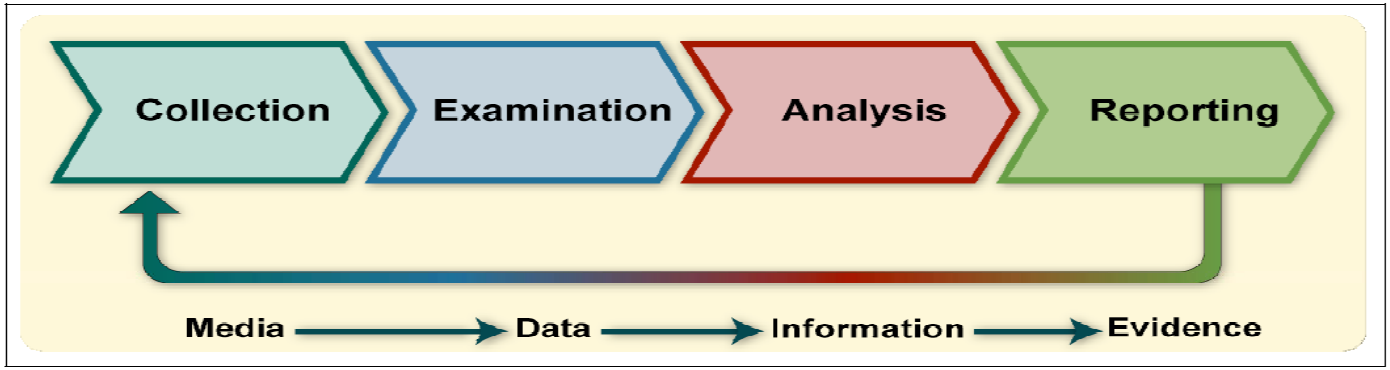
- #12. Government system boundary definitions, compartmentalization, and inventory identification
- #13. Some government-specific security requirements may not be met today in certain public cloud environments, including:
    - Least-functionality
    - Personnel security with background and nationality restrictions
    - Software development and change management

(Domain 10: Data Center Operations, Maintenance, Configuration, Physical, and Personnel Security)

Federal Cloud Security Top 20

- #14. Incident response and computer forensics in a cloud environment require fundamentally different tools, techniques, and training. Response plan must address:
  - Privacy breaches and data leakage
  - Classified spills
  - Impact to the cloud and shared cloud customers

(Domain 11: Incident Response)



Federal Cloud Security Top 20

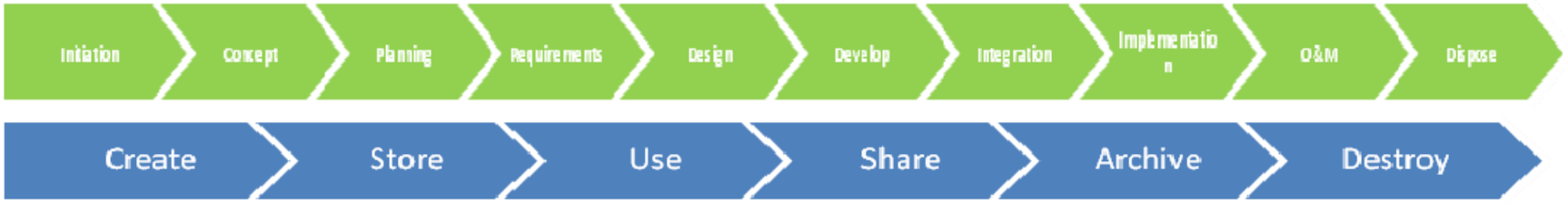
- #15. Accountability can never be outsourced from the Authorizing Official (AO). Requires:
  - Visibility to perform audits
  - Implementation robust evaluation criteria
  - Evaluate cloud security controls
- #16. New opportunities exist for real-time audit capabilities, but requires new continuous monitoring and audit technologies.

  (Domain 12: Compliance, Audit, and Accountability)

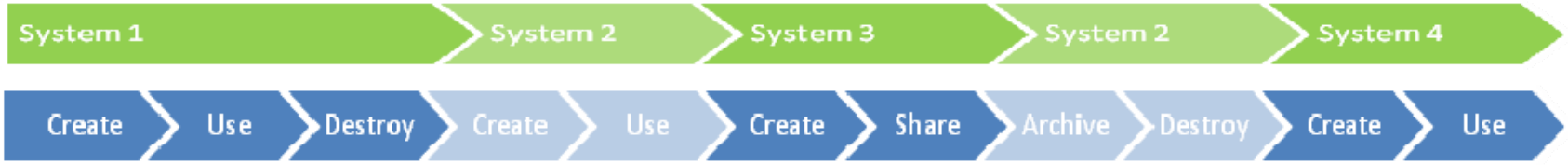
Federal Cloud Security Top 20

- #17. The System Development Life Cycle (SDLC) in a cloud requires ownership of information throughout the lifecycle.

  (Domain 13: Cloud Lifecycle Management)



System Lifecycle Management Phases



Cloud SDLC and Information Lifecycle Management Phases

Federal Cloud Security Top 20

- #18. Awareness and Training focusing on risks of information disclosure and data protection.

  (Domain 14: Awareness and Training)

- #19. Cloud compartmentalization, isolation, and system boundaries. Use of security services like Trusted Internet Connections (TIC) and DNSSEC.

  (Domain 15: System and Communication Protection)

- #20. Integrity controls vary by Service Models:
  - SaaS environments focus on application integrity and input validation
  - PaaS environments focus on API validation
  - IaaS environments focus on file system and data base integrity

  (Domain 16: System and Information Integrity)