FedRAMP Update and Lessons Learned from an Accredited 3PAO

Rob Barnes, Director, Coalfire

Governance, Risk & Compliance – G21

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
CRISC
CGEIT
CISM
CISA
2014 Fall Conference - "Think Big"

COALFIRE SENSITIVE AND PROPRIETARY.
THE INFORMATION CONTAINED IN THIS PRESENTATION IS COALFIRE SENSITIVE AND MAY NOT BE SHARED OUTSIDE OF THE COMPANY WITHOUT WRITTEN PERMISSION FROM A COALFIRE OFFICER. THIS INFORMATION IS PROTECTED BY AN NDA BETWEEN COALFIRE AND THE CLIENT.

Agenda

- **Learn**
  - History of FedRAMP
  - Who is in-process?
  - Who is certified?
- **Build**
  - FedRAMP Package
  - Key Challenges
- **Authorize**
  - Program Updates (NIST and FedRAMP)
  - Beyond FedRAMP (DIACAP, ECSB, etc.)
  - What FedRAMP Means for Your Customers
  - Current and Future Models Leveraging an ATO
- **Q&A**

UBM Tech
informationweek.com/government

InformationWeek Government

FEBRUARY 2014

Next

DOWNLOAD PDF

Cloud Security

FedRAMP

How a government program is putting cloud computing on the fast track to better security >>

By Wyatt Kash

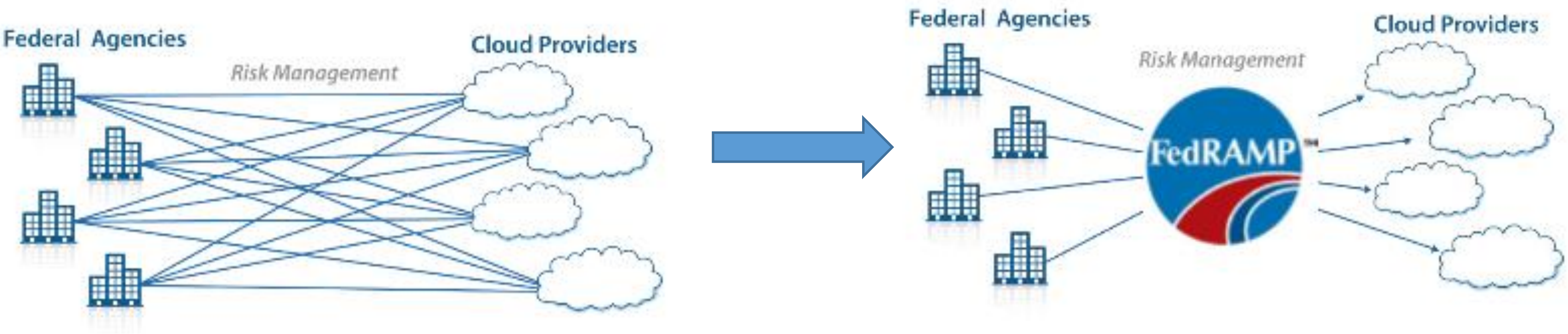
PLUS Defense CIO Teri Takai on why FedRAMP helps everyone >>

ow.ly/wLcbq

Learn

What is FedRAMP?

Federal Risk and Authorization Management Program



> *"FedRAMP establishes a standardized approach to security assessment, authorization and continuous monitoring. It will save cost, time, money and staff associated with doing this work."*
>
> **Steven Van Roekel, Federal Chief Information Officer**

Goals:

- ✓ Ensure common CSP security and compliance standards by awarding an Authority to Operate (ATO) which is accepted by all Federal Agencies
- ✓ "Do once, use many" framework

Background – Brief History of FedRAMP

OCT 2010 General Services Administration (GSA) awards first Infrastructure-as-a-Service (IaaS) Cloud Providers under a Blanket Purchase Agreement (BPA). 12 Cloud Providers were selected.

FEB 2011 White House Issues its Federal Cloud Computing Strategy "Cloud First Policy"

AUG 2011 First GSA BPA holder receives its Authority to Operate (ATO).

SEP 2011 NIST releases 800-145, "The NIST Definition of Cloud Computing". This was followed in DEC 2011 by NIST 800-144 "Guidelines on Security and Privacy in Public Cloud Computing" and in MAY 2012 by NIST 800-146 "Cloud Computing Synopsis and Recommendations."

DEC 2011 The White House releases OMB Memo "Security Authorization of Information Systems in Cloud Computing Environments" which establishes FedRAMP.

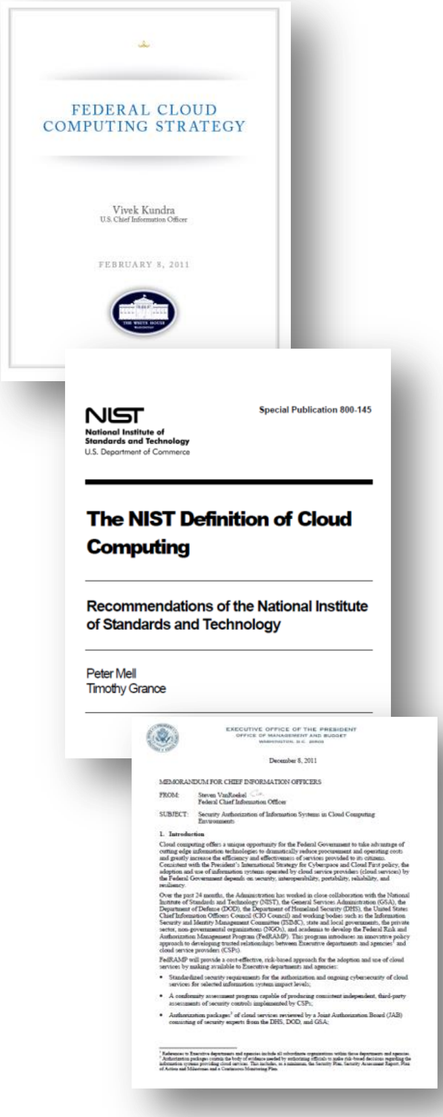
JUN 2012 FedRAMP reaches initial operating capability (IOC) in accordance with OMB FedRAMP memo timelines, and the 24 month clock starts for all clouds to meet FedRAMP requirements. FedRAMP baseline and parameters established.

JAN 2013 First CSP received FedRAMP Provisional Authorization (P-ATO).

MAR 2013 White house issues OMB M-13-9 mandating a certification in writing from the Executive department or agency CIO and CFO, a listing of all cloud services that an agency determines cannot meet the FedRAMP security authorization requirements with appropriate rationale and proposed resolutions. Quarterly updates.

JUN 2013 DISA releases a pre-solicitation for IaaS leveraging the FedRAMP requirements.

JUN 2014 All currently implemented cloud services and authorizations must meet the FedRAMP requirements.



FEDERAL CLOUD COMPUTING STRATEGY

Vivek Kundra
U.S. Chief Information Officer

FEBRUARY 8, 2011

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

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

December 8, 2011

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Steven VanRoekel
Federal Chief Information Officer

SUBJECT: Security Authorization of Information Systems in Cloud Computing Environments

1. Introduction

Cloud computing offers a unique opportunity for the Federal Government to take advantage of cutting edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens. Consistent with the President's International Strategy for Cyberspace and Cloud First policy, the adoption and use of information systems operated by cloud service providers (cloud services) by the Federal Government depends on security, interoperability, portability, reliability, and resiliency.

Over the past 24 months, the Administration has worked in close collaboration with the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), the Department of Defense (DOD), the Department of Homeland Security (DHS), the United States Chief Information Officers Council (CIO Council) and working bodies such as the Information Security and Identity Management Committee (ISIMC), state and local governments, the private sector, non-governmental organizations (NGOs), and academia to develop the Federal Risk and Authorization Management Program (FedRAMP). This program introduces an innovative policy approach to developing trusted relationships between Executive departments and agencies[1] and cloud service providers (CSPs).

FedRAMP will provide a cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies:

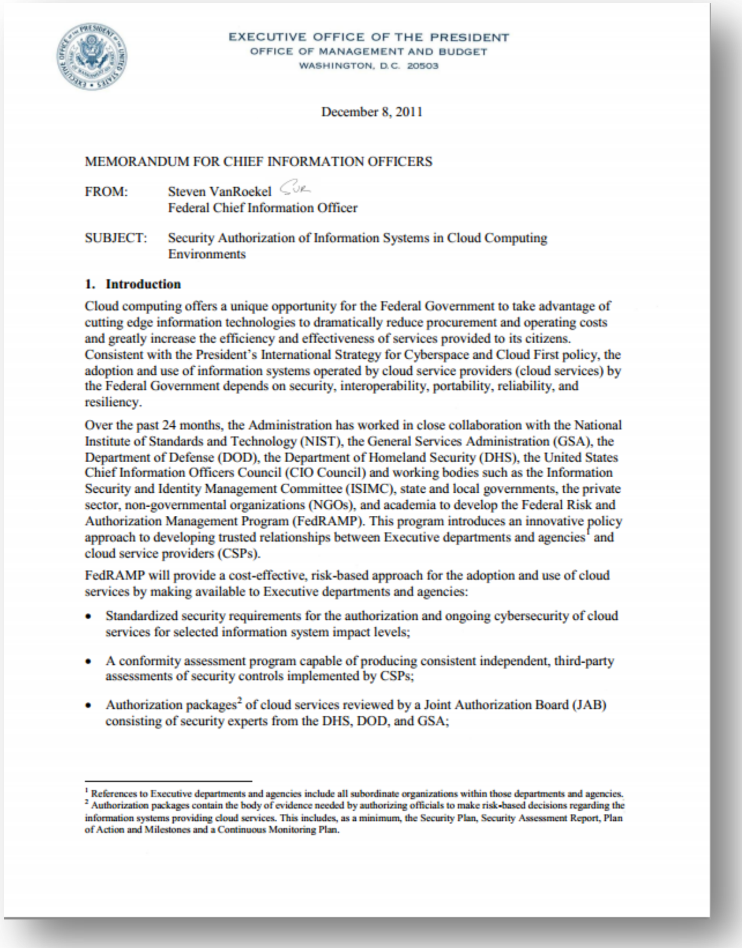
- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels;
- A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs;
- Authorization packages[2] of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the DHS, DOD, and GSA;

[1] References to Executive departments and agencies include all subordinate organizations within those departments and agencies.
[2] Authorization packages contain the body of evidence needed by authorizing officials to make risk-based decisions regarding the information systems providing cloud services. This includes, as a minimum, the Security Plan, Security Assessment Report, Plan of Action and Milestones and a Continuous Monitoring Plan.

OMB FedRAMP Policy Memo

December 8, 2011

- **Mandates FedRAMP compliance for all cloud services used by the Federal government**
  - All new services acquired after June 2012
  - All existing services by June 2014
- **Establishes Joint Authorization Board**
  - CIOs from DOD, DHS, GSA
  - Creates the FedRAMP requirements
- **Establishes PMO**
  - Maintained at GSA
  - Establishes FedRAMP processes for agency compliance
  - Maintains 3PAO program



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

December 8, 2011

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Steven VanRoekel SVR
Federal Chief Information Officer

SUBJECT: Security Authorization of Information Systems in Cloud Computing Environments

1. Introduction

Cloud computing offers a unique opportunity for the Federal Government to take advantage of cutting edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens. Consistent with the President's International Strategy for Cyberspace and Cloud First policy, the adoption and use of information systems operated by cloud service providers (cloud services) by the Federal Government depends on security, interoperability, portability, reliability, and resiliency.

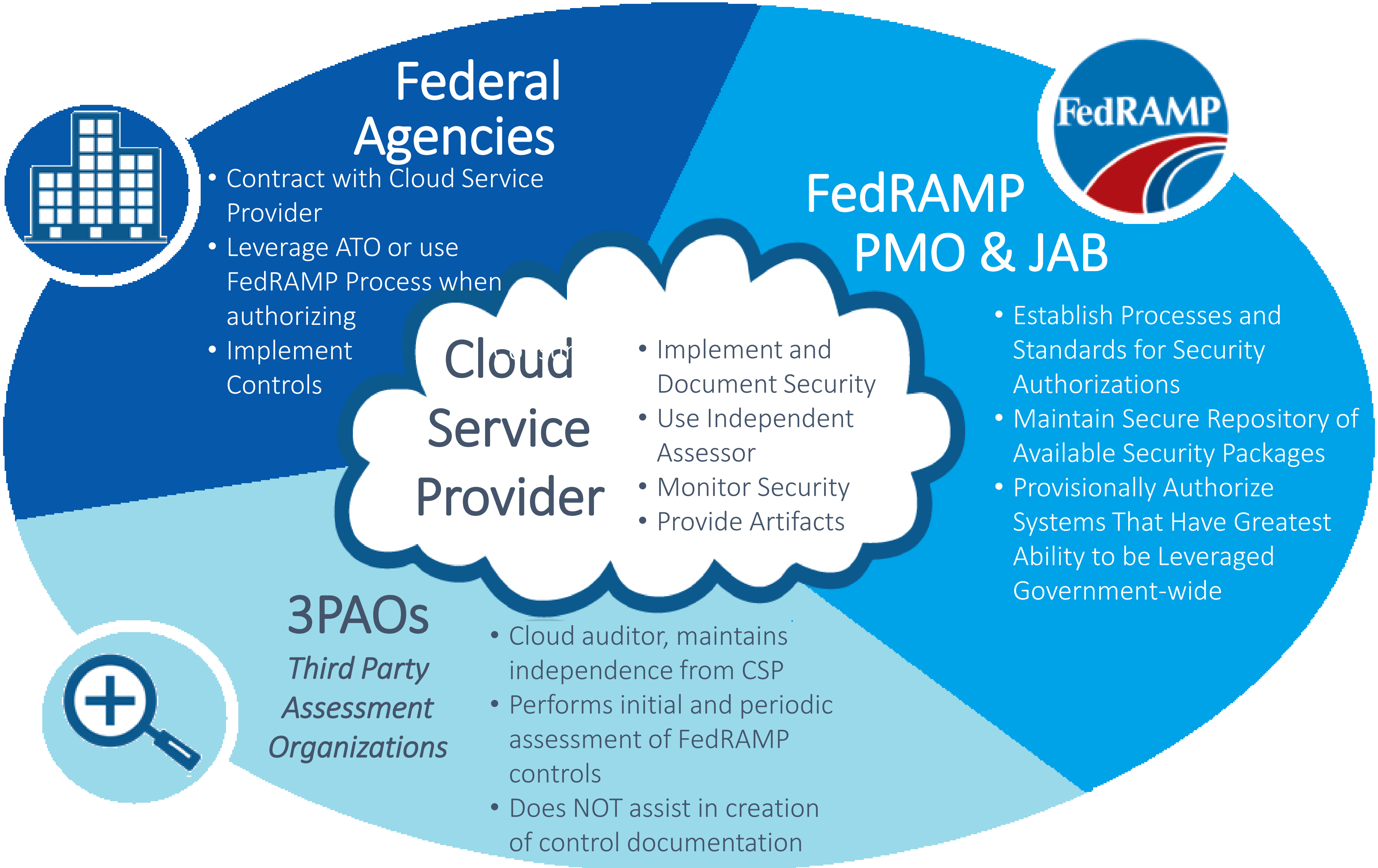
Over the past 24 months, the Administration has worked in close collaboration with the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), the Department of Defense (DOD), the Department of Homeland Security (DHS), the United States Chief Information Officers Council (CIO Council) and working bodies such as the Information Security and Identity Management Committee (ISIMC), state and local governments, the private sector, non-governmental organizations (NGOs), and academia to develop the Federal Risk and Authorization Management Program (FedRAMP). This program introduces an innovative policy approach to developing trusted relationships between Executive departments and agencies[1] and cloud service providers (CSPs).

FedRAMP will provide a cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels;
- A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs;
- Authorization packages[2] of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the DHS, DOD, and GSA;

[1] References to Executive departments and agencies include all subordinate organizations within those departments and agencies.
[2] Authorization packages contain the body of evidence needed by authorizing officials to make risk-based decisions regarding the information systems providing cloud services. This includes, as a minimum, the Security Plan, Security Assessment Report, Plan of Action and Milestones and a Continuous Monitoring Plan.

FedRAMP Key Stakeholders & Responsibilities



Federal Agencies

- Contract with Cloud Service Provider
- Leverage ATO or use FedRAMP Process when authorizing
- Implement Controls

FedRAMP PMO & JAB

- Establish Processes and Standards for Security Authorizations
- Maintain Secure Repository of Available Security Packages
- Provisionally Authorize Systems That Have Greatest Ability to be Leveraged Government-wide

Cloud Service Provider

- Implement and Document Security
- Use Independent Assessor
- Monitor Security
- Provide Artifacts

3PAOs

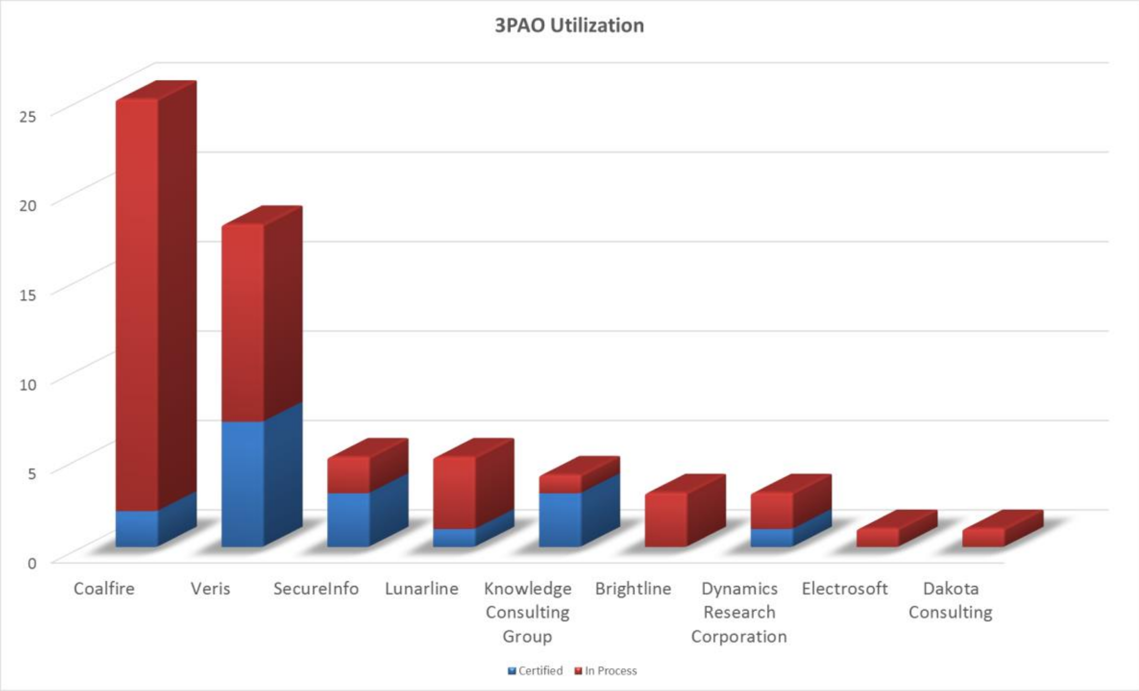
Third Party Assessment Organizations

- Cloud auditor, maintains independence from CSP
- Performs initial and periodic assessment of FedRAMP controls
- Does NOT assist in creation of control documentation

Current State of 3PAOs

Organization
Coalfire Systems
Veris Group, LLC
Lunarline, Inc.
Kratos SecureInfo
Knowledge Consulting Group, Inc.
Dynamics Research Corporation (DRC)
COACT, Inc.
BrightLine
Electrosoft Services, Inc.
Dakota Consulting, Inc.
A-lign Security and Compliance Services
Blue Canopy
Booz Allen Hamilton
Burke Consortium, Inc.
Department of Transportation Enterprise Services Center
DSD Laboratories, Inc.
Earthling Security, Inc.
EmeSec, Inc.
Excentium, Inc.
Homeland Security Consultants
Honeywell Technology Solutions, Inc.
J.D. Biggs and Associates, Inc.
KPMG, LLP
Leidos Accredtied Testing Evaluation (AT&E) Labs (formerly SAIC)
Logyx LLC
Paragon Technology Group, Inc.
PricewaterhouseCoopers LLP
SecureIT
Vencore Services and Solutions, Inc. (formerly QinetiQ North America)

- FedRAMP website – cloud.cio.gov/fedramp
- 29 accredited 3PAOs.
- Only seven 3PAO’s have successfully conducted an assessment for a FedRAMP Authorized cloud.



Tip #1

People want cloud. Cloud is seen as the only viable option.

Current State of FedRAMP CSP's

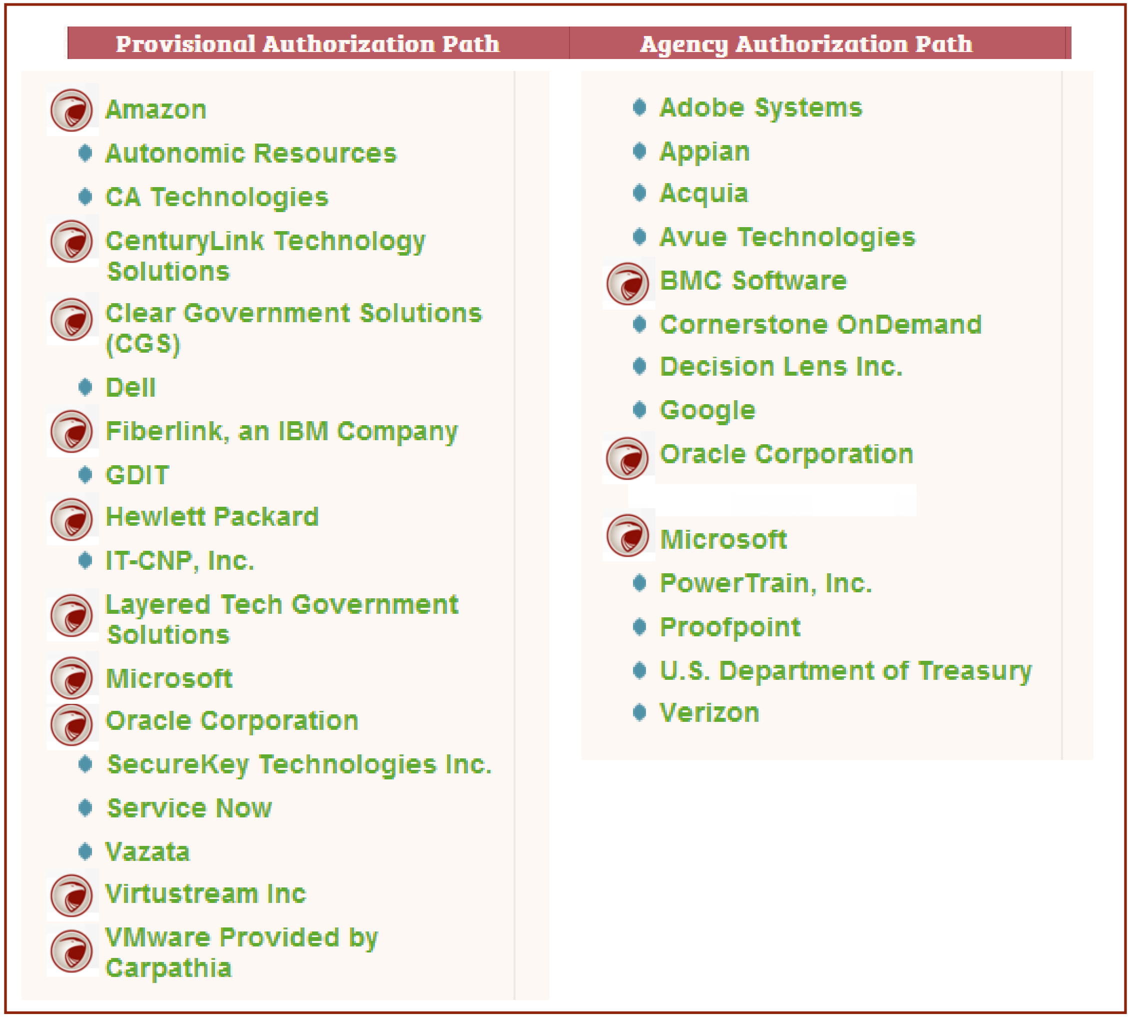
JAB FedRAMP℠ Provisional ATO

- Autonomic Resources IaaS
- CGI Federal IaaS
- AT&T StaaS IaaS
- Akamai CDN IaaS
- HP ECS-VPC IaaS
- Lockheed Martin SolaS-I IaaS
- Microsoft GFS IaaS
- Microsoft Azure PaaS
- IBM PaaS
- Oracle FMCS PaaS
- Economic Systems FHR Navigator SaaS
- CTC URHD SaaS

FedRAMP AGENCY℠ Authority to Operate

- Amazon US East West IaaS
- Amazon GovCloud IaaS
- USDA (NITC) IaaS
- HUD AINS eCase SaaS
- Salesforce Government Cloud PaaS
- MicroPact Product Suite PaaS

Current State of CSP's – In Process



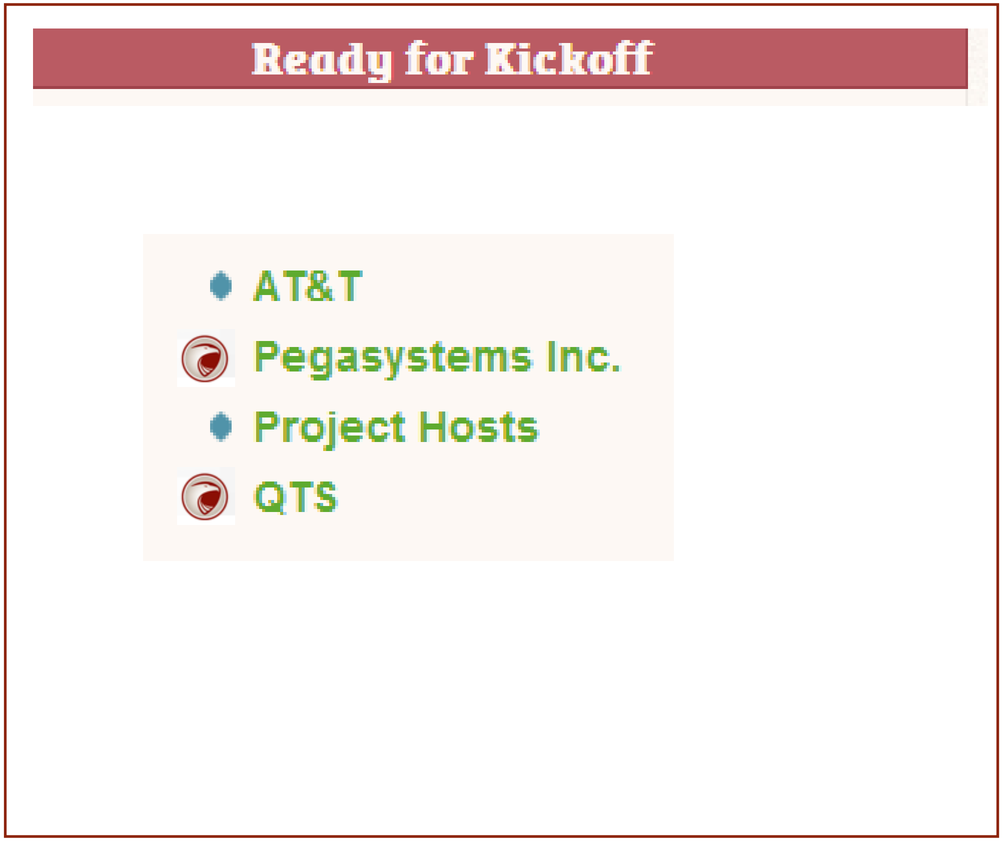
Provisional Authorization Path

- Amazon
- Autonomic Resources
- CA Technologies
- CenturyLink Technology Solutions
- Clear Government Solutions (CGS)
- Dell
- Fiberlink, an IBM Company
- GDIT
- Hewlett Packard
- IT-CNP, Inc.
- Layered Tech Government Solutions
- Microsoft
- Oracle Corporation
- SecureKey Technologies Inc.
- Service Now
- Vazata
- Virtustream Inc
- VMware Provided by Carpathia

Agency Authorization Path

- Adobe Systems
- Appian
- Acquia
- Avue Technologies
- BMC Software
- Cornerstone OnDemand
- Decision Lens Inc.
- Google
- Oracle Corporation
- Microsoft
- PowerTrain, Inc.
- Proofpoint
- U.S. Department of Treasury
- Verizon

Current State of CSP's – Ready for Kickoff



Ready for Kickoff

- AT&T
- Pegasystems Inc.
- Project Hosts
- QTS

Build

What is in a final FedRAMP package?

CSP

FedRAMP Specific

1. CIS - Control Implementation Summary
2. CTW - Control Tailoring Workbook
3. User Guide
4. E-Authentication Guide
5. FIPS 199 Categorization
6. RoB – Rules of Behavior
7. PTA & PIA - Privacy Threshold Analysis and Privacy Impact Assessment

Plans

1. SSP - System Security Plan
2. CP - Contingency Plan
3. CMP - Configuration Management Plan
4. IRP - Incident Response Plan
5. POA&M - Plan of Action and Milestones

Policies

1. Information Security Policy addressing all controls.

Procedures

1. Information Security Procedures addressing all controls

JAB/Agency

1. P-ATO Provisional Authority to Operate Memo
2. Risk Acceptance Recommendation (Optional)

3PAO

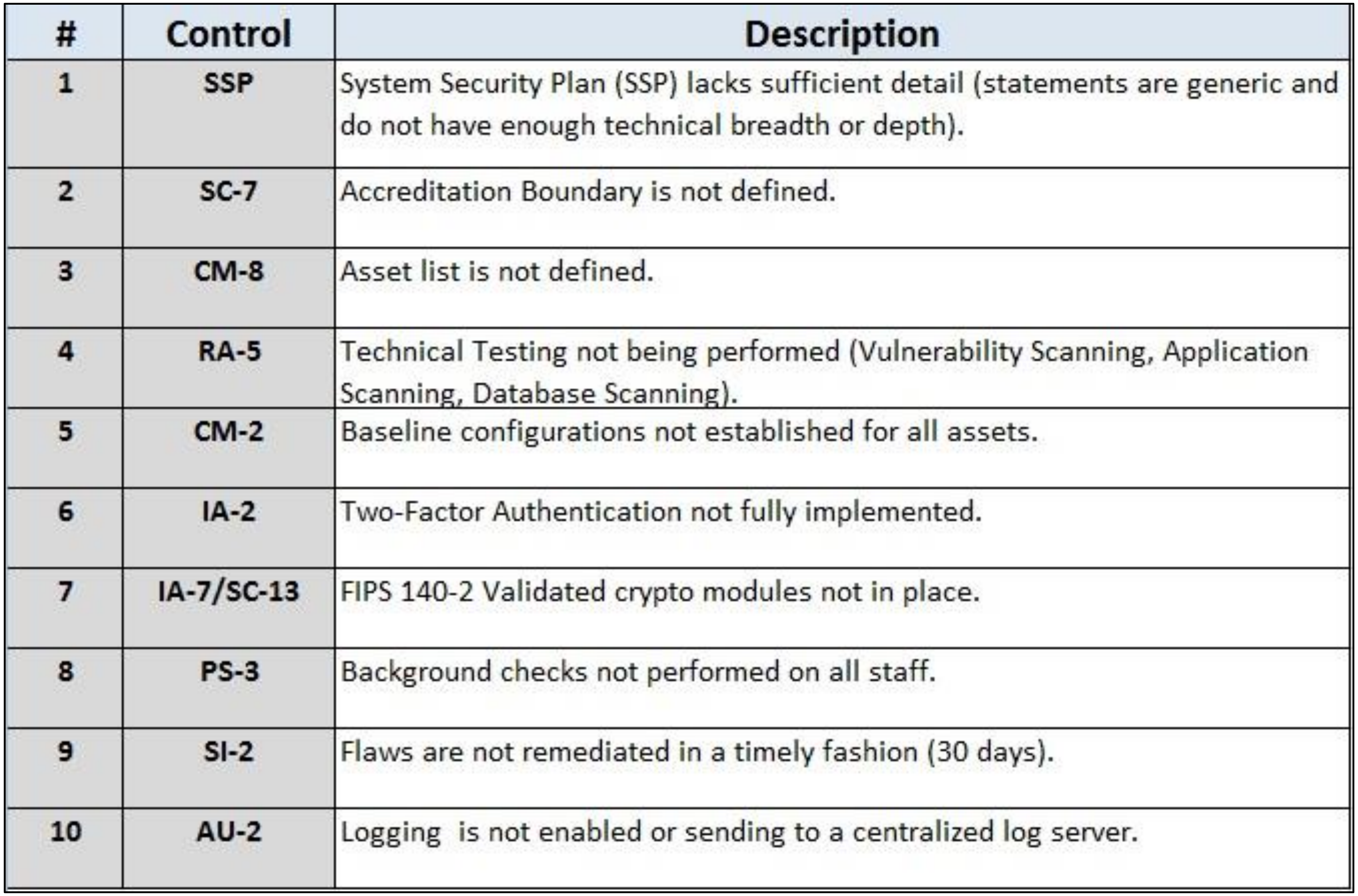
Security Tests

1. SAP – Security Assessment Plan
2. SAR – Security Assessment Report
3. SATC – Security Assessment Test Cases
4. Penetration Test
5. Infrastructure Vulnerability Scans
6. Application Vulnerability Scans
7. Database Vulnerability Scans
8. Risk Exposure Table

Tip #2

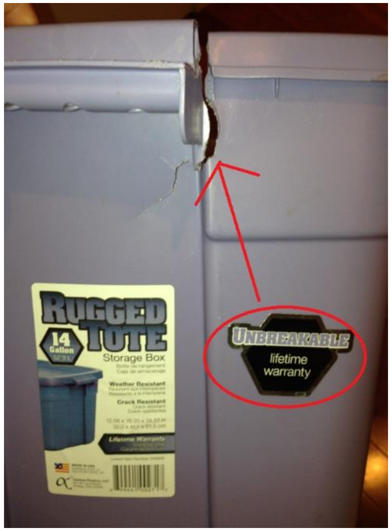
There is no high bar.
People want purpose built clouds.

Common Challenges



#	Control	Description
1	SSP	System Security Plan (SSP) lacks sufficient detail (statements are generic and do not have enough technical breadth or depth).
2	SC-7	Accreditation Boundary is not defined.
3	CM-8	Asset list is not defined.
4	RA-5	Technical Testing not being performed (Vulnerability Scanning, Application Scanning, Database Scanning).
5	CM-2	Baseline configurations not established for all assets.
6	IA-2	Two-Factor Authentication not fully implemented.
7	IA-7/SC-13	FIPS 140-2 Validated crypto modules not in place.
8	PS-3	Background checks not performed on all staff.
9	SI-2	Flaws are not remediated in a timely fashion (30 days).
10	AU-2	Logging is not enabled or sending to a centralized log server.

Authorize


RUGGED TOTE
14 Gallon
Storage Box
Weather Resistant
Crack Resistant
Lifetime Warranty
UNBREAKABLE
lifetime warranty

Agency Authority to Operate

- Organizations that meet FedRAMP requirements but receive their ATO directly from an Agency.
- Assessments performed by an accredited 3PAO.
- The 3PAO assessment process and supporting artifacts are similar to the process required to seek a JAB P-ATO.
- Other Agencies may review the CSP’s system security and issue additional Agency ATOs.

http://www.gsa.gov/portal/category/105279

JAB Provisional Authority to Operate

- Organizations that meet FedRAMP requirements and receive JAB P-ATO.
- Assessments performed by an accredited 3PAO.
- The JAB authorizes a system on behalf of the entire federal government.
- Agencies may review the CSP’s system security and issue Agency ATOs.

http://www.gsa.gov/portal/category/105279

CSP Supplied Path

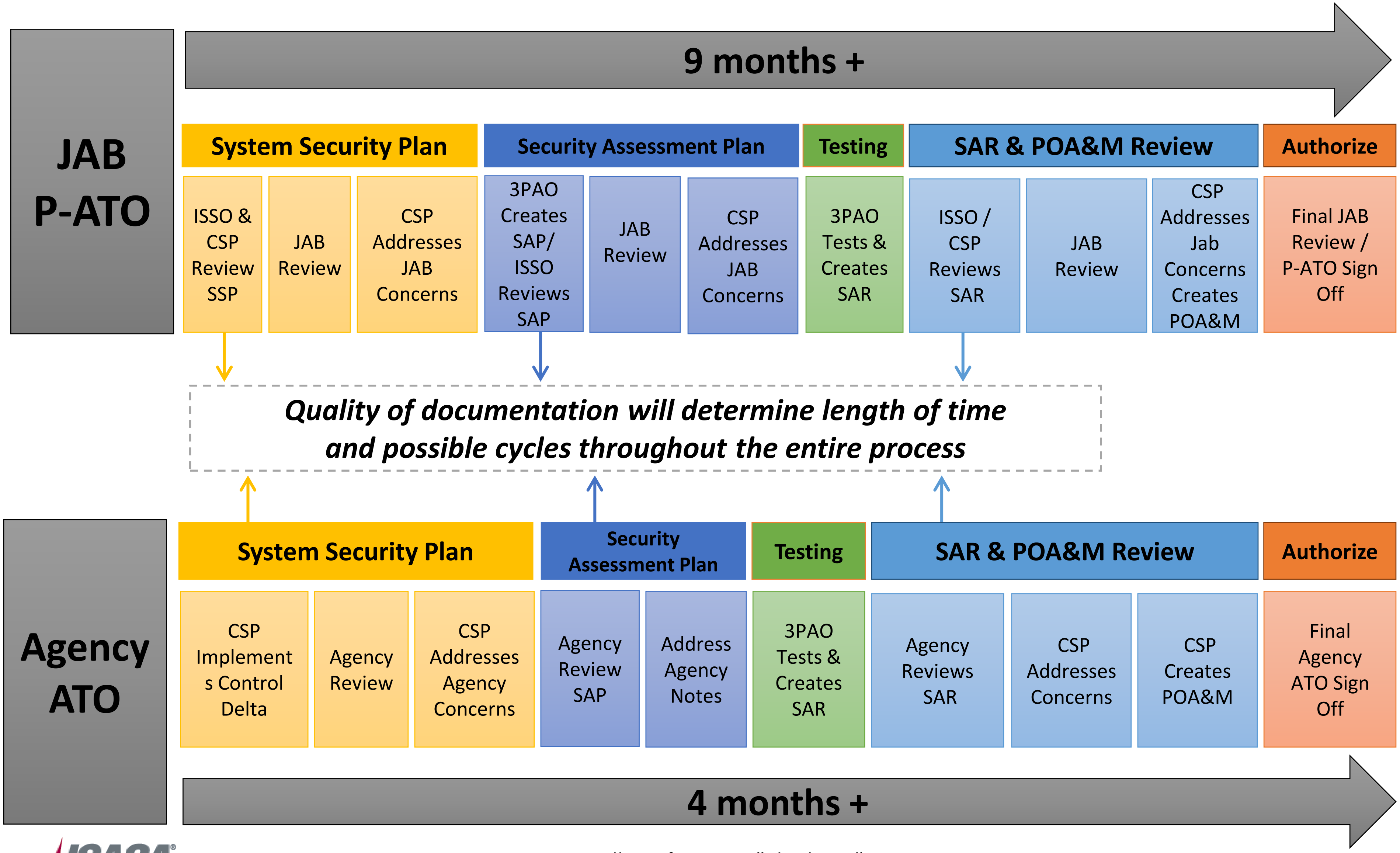
- Least common but gaining traction with major CSPs.
- FedRAMP-accredited 3PAO completes all required documentation, testing and security assessments.
- FedRAMP PMO and JAB verifies completion but does not analyze risk or issue an ATO.
- May be a high cost option due to possible additional requirements or retesting imposed by agencies who wish to procure the technology.
- May be a good option for CSPs that cannot or do not want to take advantage of existing federal contracts and do not wish to partner with other CSP’s.
- Perceived as fast path to complete the assessment process and pursue federal business.

FedRAMP
AGENCY SM
Authority to Operate

Tip #3

Transparency is key.
(Being “certified” is not enough.)

Authorization Process – JAB and Agencies



JAB P-ATO — 9 months +

System Security Plan			Security Assessment Plan			Testing	SAR & POA&M Review			Authorize
ISSO & CSP Review SSP	JAB Review	CSP Addresses JAB Concerns	3PAO Creates SAP/ ISSO Reviews SAP	JAB Review	CSP Addresses JAB Concerns	3PAO Tests & Creates SAR	ISSO / CSP Reviews SAR	JAB Review	CSP Addresses Jab Concerns Creates POA&M	Final JAB Review / P-ATO Sign Off

Quality of documentation will determine length of time and possible cycles throughout the entire process

Agency ATO — 4 months +

System Security Plan			Security Assessment Plan		Testing	SAR & POA&M Review			Authorize
CSP Implements Control Delta	Agency Review	CSP Addresses Agency Concerns	Agency Review SAP	Address Agency Notes	3PAO Tests & Creates SAR	Agency Reviews SAR	CSP Addresses Concerns	CSP Creates POA&M	Final Agency ATO Sign Off

JAB Provisional ATO vs Agency ATO

Timeframe

- JAB 25+ weeks minimum
- Agency 14+ weeks minimum

Level / Depth of Review

- JAB: Four sets of eyes (PMO, DoD, DHS, GSA)
- Agency: Sponsoring agency review

Risk Acceptance Level

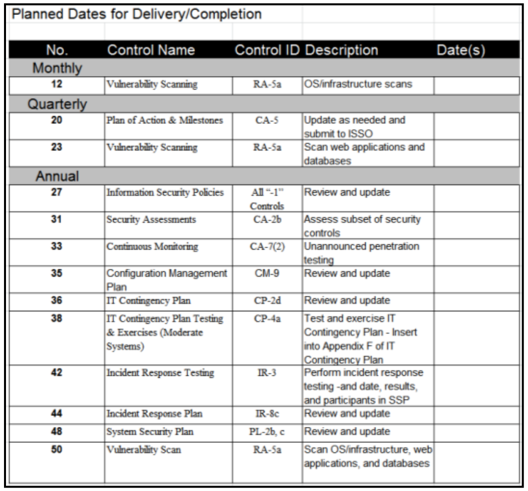
- JAB: Low risk tolerance level, security for security
- Agency: Varying levels of risk acceptance, business needs can justify more risk as can individual agency policies

Continuous Monitoring

- JAB: JAB/PMO will maintain, agencies need to review
- Agency: Agency must work with CSP to complete

Continuous Monitoring

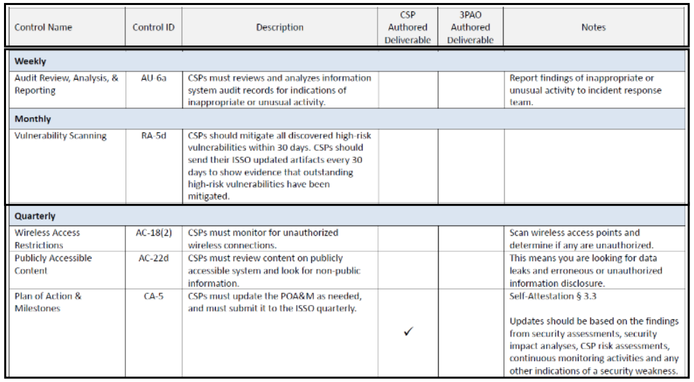
- Upon issue of the P-ATO, the CSP and 3PAO establish dates.



Planned Dates for Delivery/Completion

No.	Control Name	Control ID	Description	Date(s)
Monthly				
12	Vulnerability Scanning	RA-5a	OS/infrastructure scans	
Quarterly				
20	Plan of Action & Milestones	CA-5	Update as needed and submit to ISSO	
23	Vulnerability Scanning	RA-5a	Scan web applications and databases	
Annual				
27	Information Security Policies	All "-1" Controls	Review and update	
31	Security Assessments	CA-2b	Assess subset of security controls	
33	Continuous Monitoring	CA-7(2)	Unannounced penetration testing	
35	Configuration Management Plan	CM-9	Review and update	
36	IT Contingency Plan	CP-2d	Review and update	
38	IT Contingency Plan Testing & Exercises (Moderate Systems)	CP-4a	Test and exercise IT Contingency Plan - Insert into Appendix F of IT Contingency Plan	
42	Incident Response Testing	IR-3	Perform incident response testing -and date, results, and participants in SSP	
44	Incident Response Plan	IR-8c	Review and update	
48	System Security Plan	PL-2b, c	Review and update	
50	Vulnerability Scan	RA-5a	Scan OS/infrastructure, web applications, and databases	

- **Identify key dates:**
  - P-ATO issue
  - POA&M Actions
  - Annual Assessment
- **Submitted through the ISSO.**
- **CSP and 3PAO should agree to dates that impact both organizations.**



Control Name	Control ID	Description	CSP Authored Deliverable	3PAO Authored Deliverable	Notes
Weekly					
Audit Review, Analysis, & Reporting	AU-6a	CSPs must reviews and analyzes information system audit records for indications of inappropriate or unusual activity.			Report findings of inappropriate or unusual activity to incident response team.
Monthly					
Vulnerability Scanning	RA-5d	CSPs should mitigate all discovered high-risk vulnerabilities within 30 days. CSPs should send their ISSO updated artifacts every 30 days to show evidence that outstanding high-risk vulnerabilities have been mitigated.			
Quarterly					
Wireless Access Restrictions	AC-18(2)	CSPs must monitor for unauthorized wireless connections.			Scan wireless access points and determine if any are unauthorized.
Publicly Accessible Content	AC-22d	CSPs must review content on publicly accessible system and look for non-public information.			This means you are looking for data leaks and erroneous or unauthorized information disclosure.
Plan of Action & Milestones	CA-5	CSPs must update the POA&M as needed, and must submit it to the ISSO quarterly.	✓		Self-Attestation § 3.3 Updates should be based on the findings from security assessments, security impact analyses, CSP risk assessments, continuous monitoring activities and any other indications of a security weakness.

- **Requirements for CSP and 3PAO.**
- **Annual Assessment:**
  - Sample Controls
  - Penetration Test
  - Vulnerability Scans

Predicting the Future: FedRAMP Maturity

- Release of 800-53 Rev 4 Baseline and Documentation
  - Cloud First deadline was June 6th – 2 Year anniversary for FedRAMP
  - 325 Controls for FedRAMP Moderate – Increase from 298
  - Documentation templates updated
  - Migration is happening now, but most CSPs will transition in 2015
    - Continuous Monitoring / Annual Assessment
- CSP Supplied Path
  - Significant backlog and wait time associated with the JAB path
    - 12-18 months total wait time
    - 9 months once ready for kickoff
  - Agencies are hesitant to sponsor CSPs – cost / benefit
  - Major players are initiating CSP Supplied path
    - Potential loss of business
    - FedRAMP identified as required in new RFPs

> **“The reality is, the government is not going to function without this technology.”**
>
> Robert Barnes, Director, Public Sector Practice Leader, Coalfire Systems Inc.

Future: NIST SP 800-53 Revision 4 and FedRAMP

- Release of 800-53 Rev 4 Baseline and Documentation
  - Deadline was June 6th – 2 Year anniversary for FedRAMP
  - New baseline controls - Text format, workbook expected by October 1, 2014.
  - 325 Controls for FedRAMP Moderate – Increase from 298
  - Major documentation update – Templates available on FedRAMP website

- Transition Strategy
  - Rev. 4 Released April 22, 2013
  - CSPs divided in to 3 categories - Initiation, In Process, Continuous Monitoring
  - Update of controls and documentation
  - Testing timeframes
  - Transition Plan to be released with documentation updates

Impact System Level	Controls in Rev 3	Controls in Rev 4
Low-	115	124
Moderate-	252	261
High-	329	343

Is my organization required to transition?

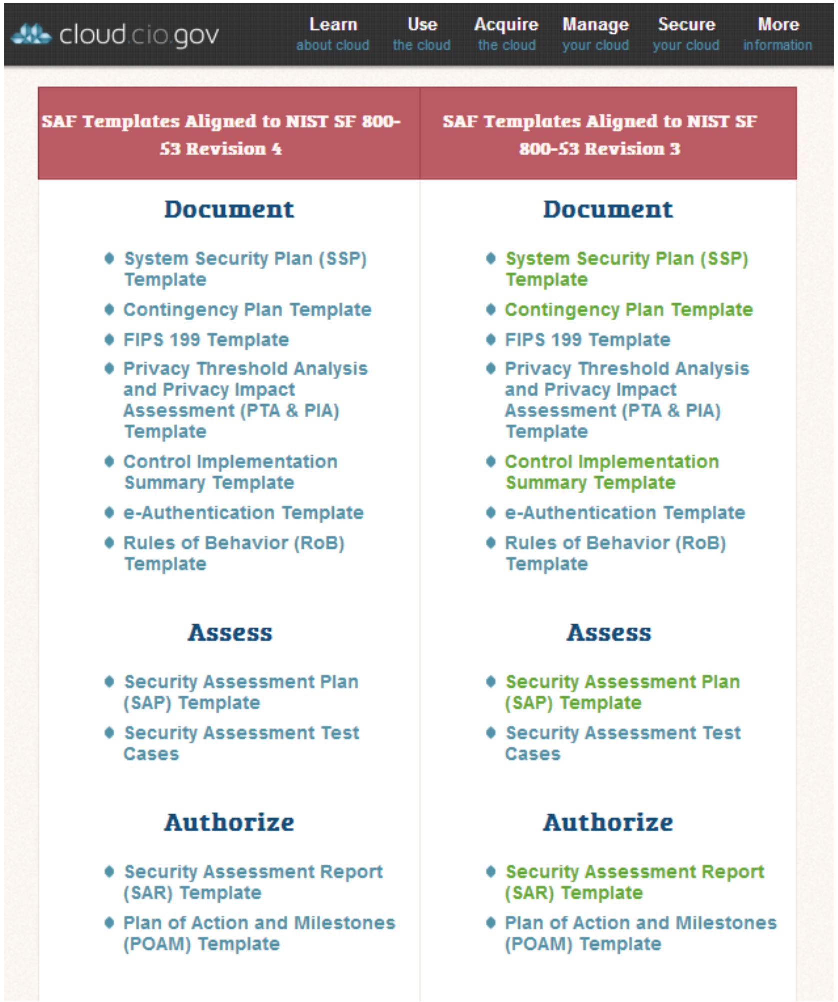
You must transition to NIST SP 800-53 Rev 4 if you do not meet any of the following criteria:

- Kicked off JAB P-ATO review prior to June 1, 2014.
- In Agency ATO review prior to June 1, 2014.
- In contract discussions with Agencies.
- In contract with an Agency prior to June 1, 2014.

This is not intended to be disruptive or to prevent those in process from having to change course.

Download the Templates

- http://cloud.cio.gov/fedramp/templates



SAF Templates Aligned to NIST SF 800-53 Revision 4

Document

- System Security Plan (SSP) Template
- Contingency Plan Template
- FIPS 199 Template
- Privacy Threshold Analysis and Privacy Impact Assessment (PTA & PIA) Template
- Control Implementation Summary Template
- e-Authentication Template
- Rules of Behavior (RoB) Template

Assess

- Security Assessment Plan (SAP) Template
- Security Assessment Test Cases

Authorize

- Security Assessment Report (SAR) Template
- Plan of Action and Milestones (POAM) Template

SAF Templates Aligned to NIST SF 800-53 Revision 3

Document

- System Security Plan (SSP) Template
- Contingency Plan Template
- FIPS 199 Template
- Privacy Threshold Analysis and Privacy Impact Assessment (PTA & PIA) Template
- Control Implementation Summary Template
- e-Authentication Template
- Rules of Behavior (RoB) Template

Assess

- Security Assessment Plan (SAP) Template
- Security Assessment Test Cases

Authorize

- Security Assessment Report (SAR) Template
- Plan of Action and Milestones (POAM) Template

Tip #4

Early adopters are maximizing their investment.

Leveraging a FedRAMP Authorized Cloud Solution

- SaaS providers will leverage authorizations of IaaS/PaaS providers.
- PaaS providers will leverage authorizations of IaaS providers.
- FedRAMP PMO – Guide to Understanding FedRAMP has an entire section dedicated to Agencies wanting to leverage services from multiple providers and how each provider's Authorization relates to the other.

http://www.gsa.gov/portal/mediaId/170599/fileName/Guide_to_Understanding_FedRAMP_042213

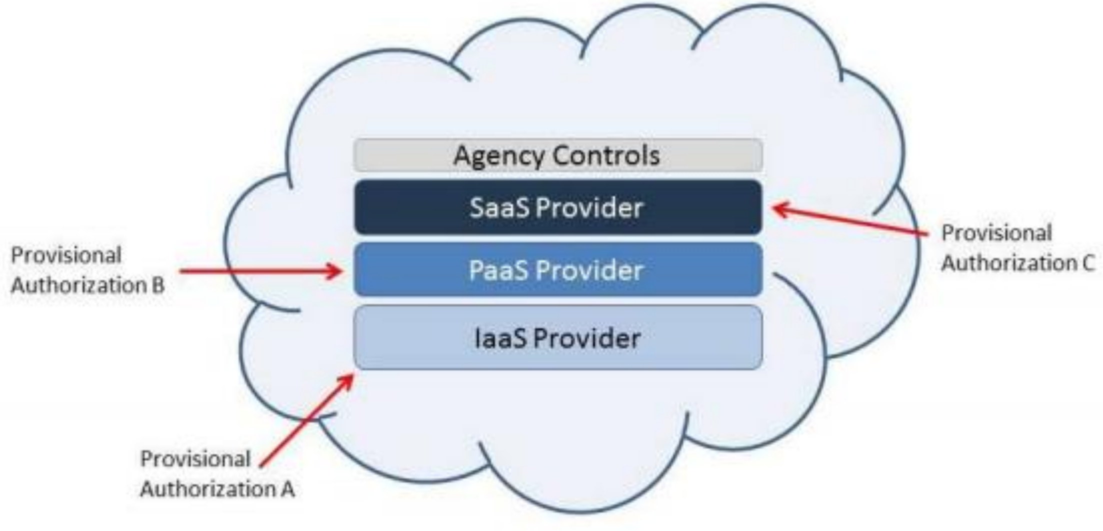

Agency Controls
SaaS Provider
PaaS Provider
IaaS Provider
Provisional Authorization C
Provisional Authorization B
Provisional Authorization A

Figure 3-12. Three Providers, One IaaS, One PaaS, and One SaaS

Beyond FedRAMP

- 80% of Coalfire's FedRAMP customers meet multiple requirements

Acronym	Requirement
FISMA HIGH	Federal Information Systems Management Act
HHS, GSA, VA	Agency Specific Requirements and RFPs
ECSB	Defense Information Systems Agency (DISA) Enterprise Cloud Service Broker
DIACAP	Defense Information Assurance Certification and Accreditation Program
DoD RMF	Defense Information Assurance Risk Management Process
CJIS	Criminal Justice Information System
ISO 27001	International Organization of Standardization - Info Sec Management System
PCI DSS	Payment Card Industry Data Security Standard
HIPAA	Health Insurance Portability and Accountability Act

Tip #5

Risk management processes matter, not the controls frameworks.

Controls Frameworks – Mapping

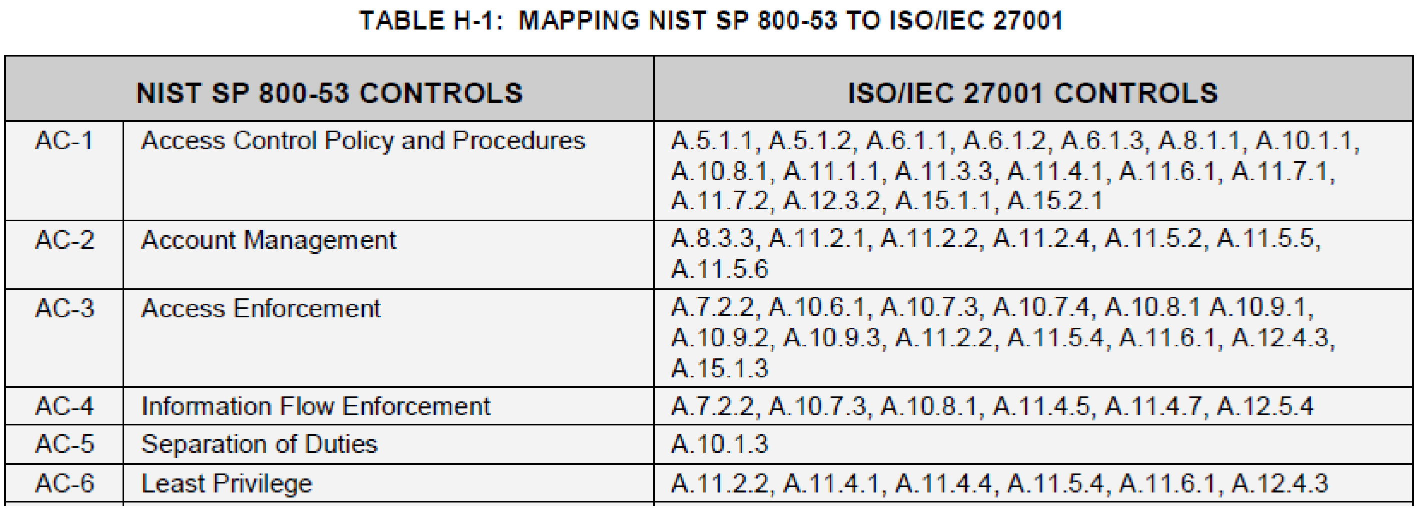


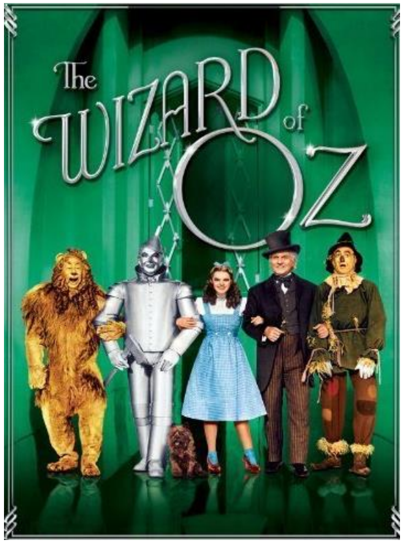
TABLE H-1: MAPPING NIST SP 800-53 TO ISO/IEC 27001

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
AC-1	Access Control Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.8.1, A.11.1.1, A.11.3.3, A.11.4.1, A.11.6.1, A.11.7.1, A.11.7.2, A.12.3.2, A.15.1.1, A.15.2.1
AC-2	Account Management	A.8.3.3, A.11.2.1, A.11.2.2, A.11.2.4, A.11.5.2, A.11.5.5, A.11.5.6
AC-3	Access Enforcement	A.7.2.2, A.10.6.1, A.10.7.3, A.10.7.4, A.10.8.1 A.10.9.1, A.10.9.2, A.10.9.3, A.11.2.2, A.11.5.4, A.11.6.1, A.12.4.3, A.15.1.3
AC-4	Information Flow Enforcement	A.7.2.2, A.10.7.3, A.10.8.1, A.11.4.5, A.11.4.7, A.12.5.4
AC-5	Separation of Duties	A.10.1.3
AC-6	Least Privilege	A.11.2.2, A.11.4.1, A.11.4.4, A.11.5.4, A.11.6.1, A.12.4.3

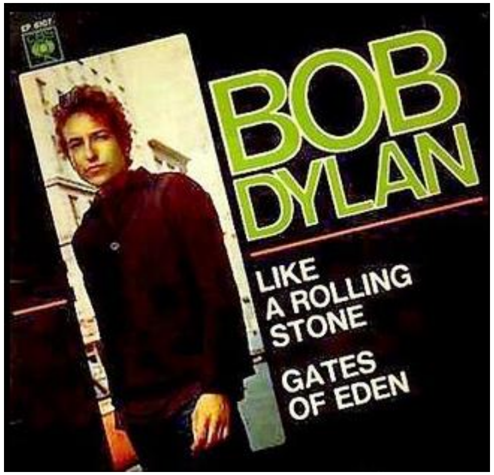
It's a bit painful to do the mapping, but its doable…

Controls Mapping - FedRAMP

- NIST formalized the concept of “control overlays”
- FedRAMP is a Cloud control overlay to NIST 800-53
- Control overlays are used to tailor a baseline of controls to a specific industry/technology/group of similar interests.
- Company’s try to meet the HIGH bar, be the best!



Best movie ever!
Rotten Tomatoes

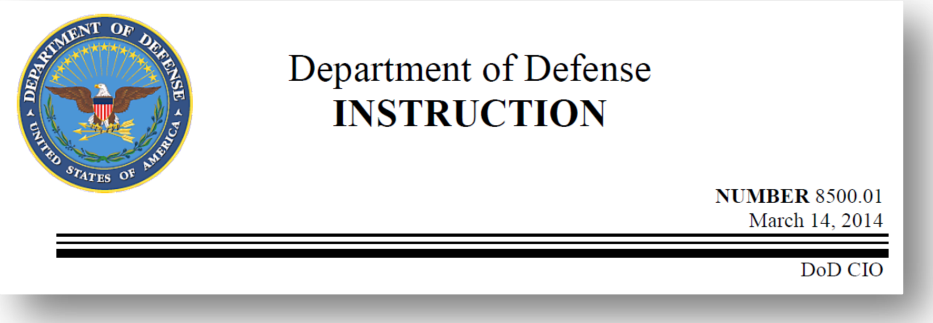


Best song ever!
Rolling Stone

Lamborghini Murcielago

Best car ever!
Top Gear

DoD Changes?



Department of Defense
INSTRUCTION

NUMBER 8500.01
March 14, 2014

DoD CIO

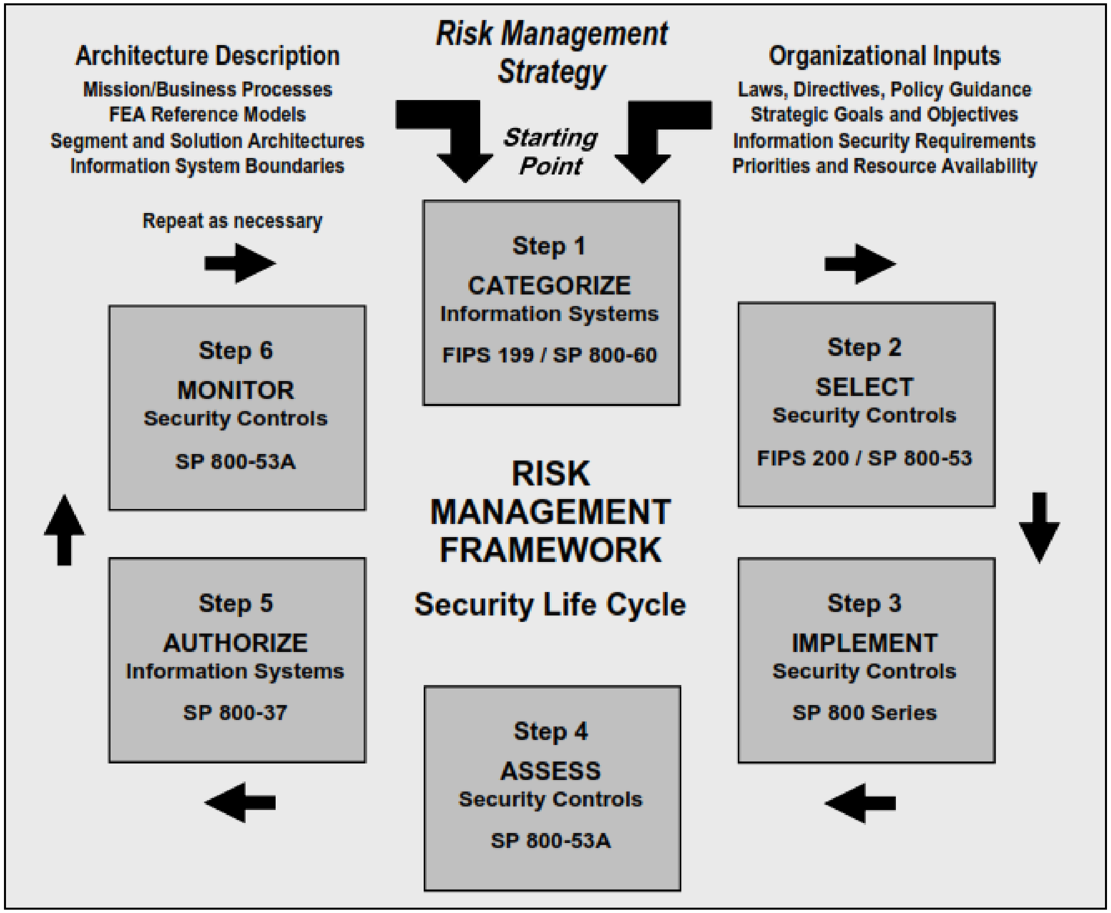
- **RMF**

DoD will use NIST SP 800-37 ("Guide for Applying the Risk Management Framework to Federal Information Systems"), as implemented by [...] DoD Instruction 8510.01 ("Risk Management Framework (RMF) for DoD Information Technology (IT)", March 13, 2014) to address risk management, including authorization to operate (ATO), for all DoD ISs and PIT systems."

- **Reciprocity**

DoD Components must share security authorization packages with affected information owners (IOs) or stewards and interconnected ISOs to support Cybersecurity reciprocity. The reciprocal acceptance of DoD and other federal agency and department security authorizations will be implemented in accordance with the procedures in DoD Instruction 8510.01 (RFM for DoD IT - March 13, 2014)

What is the RMF?



Risk Management Strategy

Architecture Description

Mission/Business Processes
FEA Reference Models
Segment and Solution Architectures
Information System Boundaries

Organizational Inputs

Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Information Security Requirements
Priorities and Resource Availability

Starting Point

Repeat as necessary

Step 1
CATEGORIZE
Information Systems
FIPS 199 / SP 800-60

Step 2
SELECT
Security Controls
FIPS 200 / SP 800-53

Step 3
IMPLEMENT
Security Controls
SP 800 Series

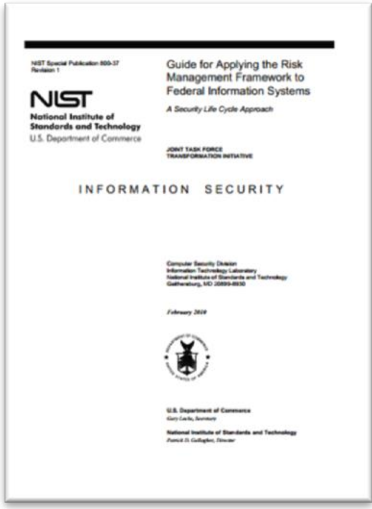
Step 4
ASSESS
Security Controls
SP 800-53A

Step 5
AUTHORIZE
Information Systems
SP 800-37

Step 6
MONITOR
Security Controls
SP 800-53A

RISK MANAGEMENT FRAMEWORK

Security Life Cycle



NIST Special Publication 800-37
Revision 1

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

Guide for Applying the Risk Management Framework to Federal Information Systems

A Security Life Cycle Approach

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

NIST SP 800-30
NIST SP 800-37

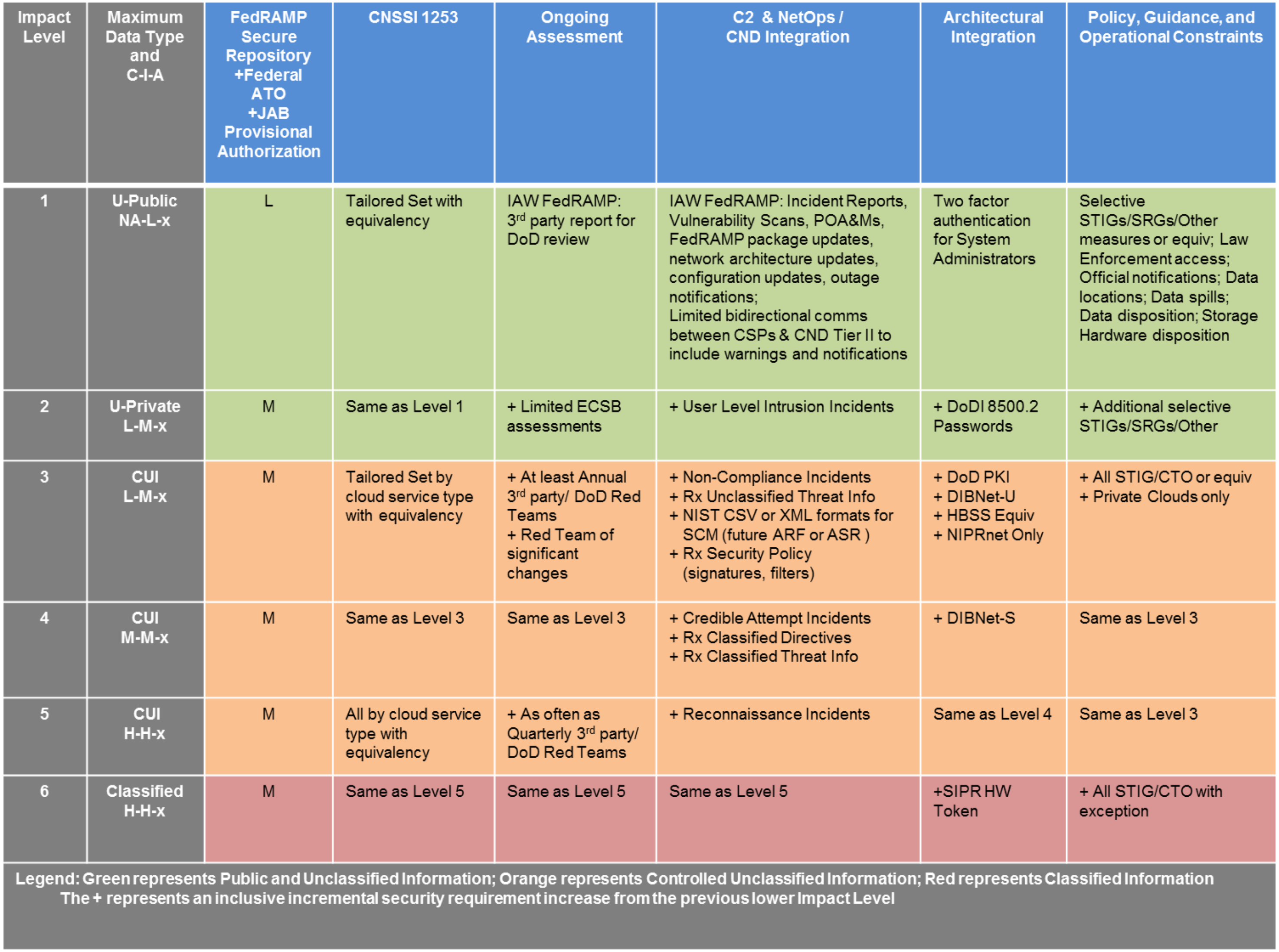
Control Frameworks – NIST

- All NIST documents are freely available and updated by the US Government.
- Does not prohibit cloud adoption and the flexibility in technical control selection makes it very powerful, but,
- NIST doesn't define any control REQUIREMENTS.

ex: Passwords must meet [AGENCY DEFINED] requirements.

- Assessment to NIST has been wide and varied.

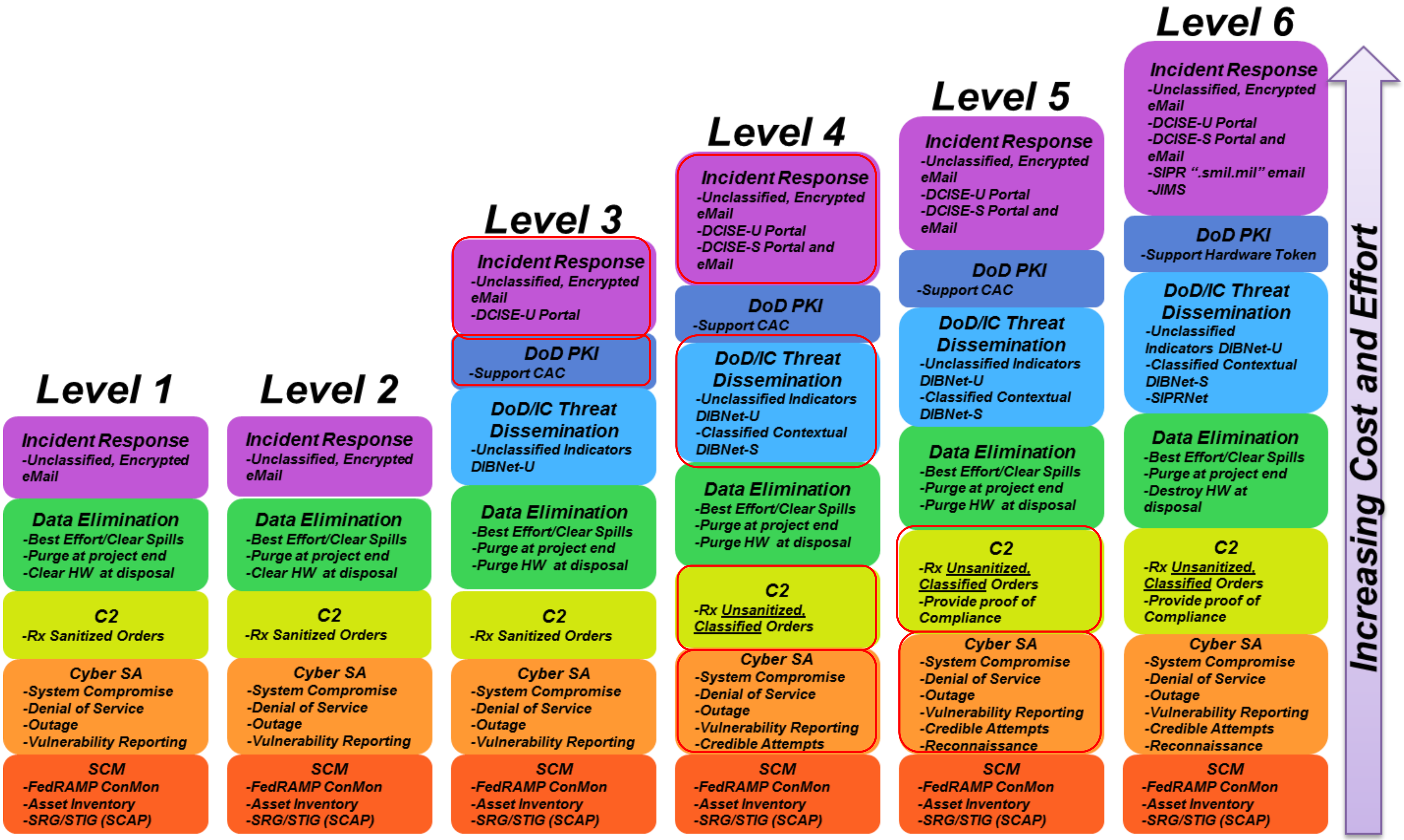
What is the ECSB? - Impact Levels



Impact Level	Maximum Data Type and C-I-A	FedRAMP Secure Repository +Federal ATO +JAB Provisional Authorization	CNSSI 1253	Ongoing Assessment	C2 & NetOps / CND Integration	Architectural Integration	Policy, Guidance, and Operational Constraints
1	U-Public NA-L-x	L	Tailored Set with equivalency	IAW FedRAMP: 3rd party report for DoD review	IAW FedRAMP: Incident Reports, Vulnerability Scans, POA&Ms, FedRAMP package updates, network architecture updates, configuration updates, outage notifications; Limited bidirectional comms between CSPs & CND Tier II to include warnings and notifications	Two factor authentication for System Administrators	Selective STIGs/SRGs/Other measures or equiv; Law Enforcement access; Official notifications; Data locations; Data spills; Data disposition; Storage Hardware disposition
2	U-Private L-M-x	M	Same as Level 1	+ Limited ECSB assessments	+ User Level Intrusion Incidents	+ DoDI 8500.2 Passwords	+ Additional selective STIGs/SRGs/Other
3	CUI L-M-x	M	Tailored Set by cloud service type with equivalency	+ At least Annual 3rd party/ DoD Red Teams + Red Team of significant changes	+ Non-Compliance Incidents + Rx Unclassified Threat Info + NIST CSV or XML formats for SCM (future ARF or ASR) + Rx Security Policy (signatures, filters)	+ DoD PKI + DIBNet-U + HBSS Equiv + NIPRnet Only	+ All STIG/CTO or equiv + Private Clouds only
4	CUI M-M-x	M	Same as Level 3	Same as Level 3	+ Credible Attempt Incidents + Rx Classified Directives + Rx Classified Threat Info	+ DIBNet-S	Same as Level 3
5	CUI H-H-x	M	All by cloud service type with equivalency	+ As often as Quarterly 3rd party/ DoD Red Teams	+ Reconnaissance Incidents	Same as Level 4	Same as Level 3
6	Classified H-H-x	M	Same as Level 5	Same as Level 5	Same as Level 5	+SIPR HW Token	+ All STIG/CTO with exception

Legend: Green represents Public and Unclassified Information; Orange represents Controlled Unclassified Information; Red represents Classified Information
The + represents an inclusive incremental security requirement increase from the previous lower Impact Level

What is the ECSB? – (cont)



Level 1

Incident Response
-Unclassified, Encrypted eMail

Data Elimination
-Best Effort/Clear Spills
-Purge at project end
-Clear HW at disposal

C2
-Rx Sanitized Orders

Cyber SA
-System Compromise
-Denial of Service
-Outage
-Vulnerability Reporting

SCM
-FedRAMP ConMon
-Asset Inventory
-SRG/STIG (SCAP)

Level 2

Incident Response
-Unclassified, Encrypted eMail

Data Elimination
-Best Effort/Clear Spills
-Purge at project end
-Clear HW at disposal

C2
-Rx Sanitized Orders

Cyber SA
-System Compromise
-Denial of Service
-Outage
-Vulnerability Reporting

SCM
-FedRAMP ConMon
-Asset Inventory
-SRG/STIG (SCAP)

Level 3

Incident Response
-Unclassified, Encrypted eMail
-DCISE-U Portal

DoD PKI
-Support CAC

DoD/IC Threat Dissemination
-Unclassified Indicators DIBNet-U

Data Elimination
-Best Effort/Clear Spills
-Purge at project end
-Purge HW at disposal

C2
-Rx Sanitized Orders

Cyber SA
-System Compromise
-Denial of Service
-Outage
-Vulnerability Reporting

SCM
-FedRAMP ConMon
-Asset Inventory
-SRG/STIG (SCAP)

Level 4

Incident Response
-Unclassified, Encrypted eMail
-DCISE-U Portal
-DCISE-S Portal and eMail

DoD PKI
-Support CAC

DoD/IC Threat Dissemination
-Unclassified Indicators DIBNet-U
-Classified Contextual DIBNet-S

Data Elimination
-Best Effort/Clear Spills
-Purge at project end
-Purge HW at disposal

C2
-Rx Unsanitized, Classified Orders

Cyber SA
-System Compromise
-Denial of Service
-Outage
-Vulnerability Reporting
-Credible Attempts

SCM
-FedRAMP ConMon
-Asset Inventory
-SRG/STIG (SCAP)

Level 5

Incident Response
-Unclassified, Encrypted eMail
-DCISE-U Portal
-DCISE-S Portal and eMail

DoD PKI
-Support CAC

DoD/IC Threat Dissemination
-Unclassified Indicators DIBNet-U
-Classified Contextual DIBNet-S

Data Elimination
-Best Effort/Clear Spills
-Purge at project end
-Purge HW at disposal

C2
-Rx Unsanitized, Classified Orders
-Provide proof of Compliance

Cyber SA
-System Compromise
-Denial of Service
-Outage
-Vulnerability Reporting
-Credible Attempts
-Reconnaissance

SCM
-FedRAMP ConMon
-Asset Inventory
-SRG/STIG (SCAP)

Level 6

Incident Response
-Unclassified, Encrypted eMail
-DCISE-U Portal
-DCISE-S Portal and eMail
-SIPR ".smil.mil" email
-JIMS

DoD PKI
-Support Hardware Token

DoD/IC Threat Dissemination
-Unclassified Indicators DIBNet-U
-Classified Contextual DIBNet-S
-SIPRNet

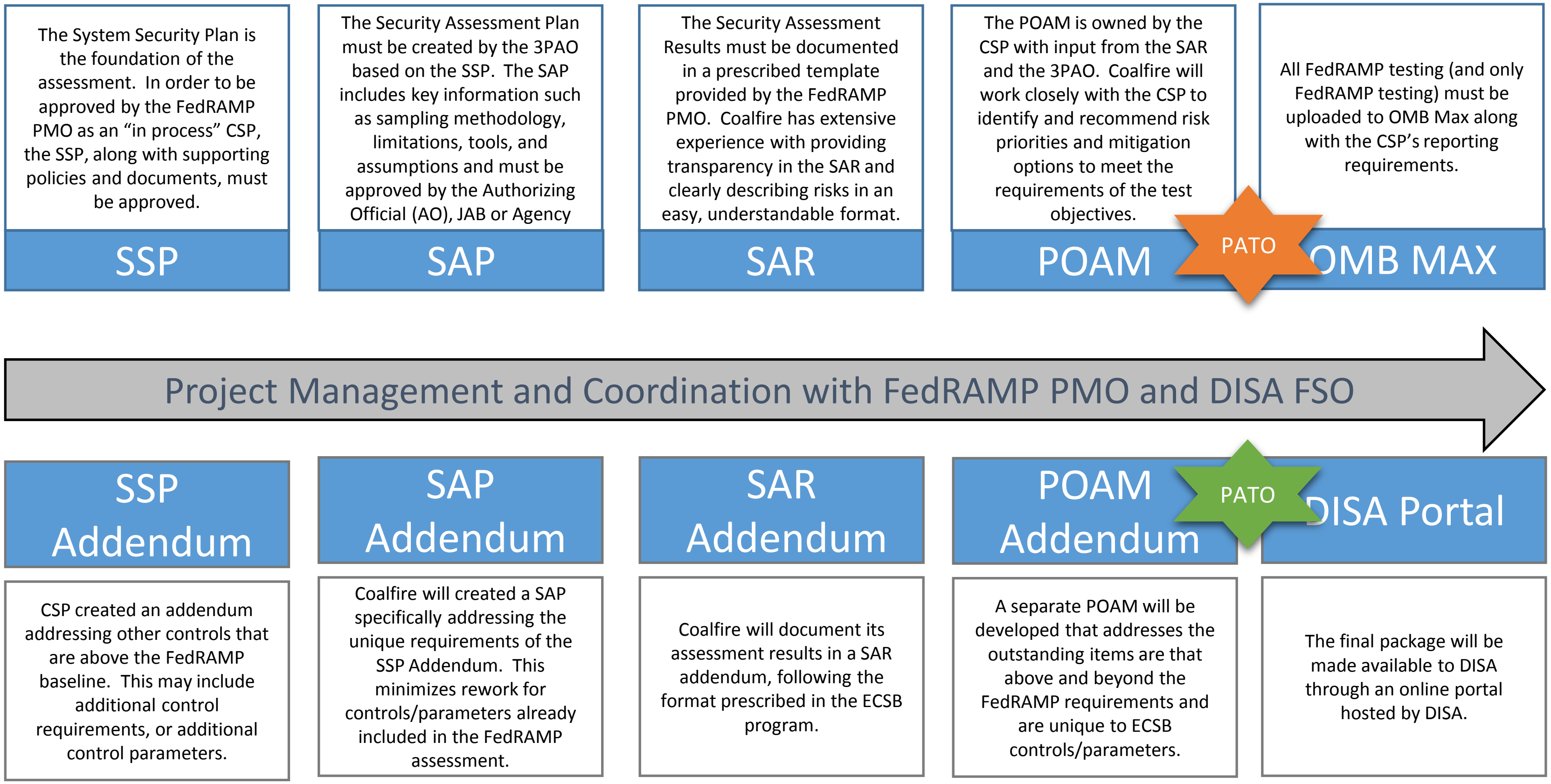
Data Elimination
-Best Effort/Clear Spills
-Purge at project end
-Destroy HW at disposal

C2
-Rx Unsanitized, Classified Orders
-Provide proof of Compliance

Cyber SA
-System Compromise
-Denial of Service
-Outage
-Vulnerability Reporting
-Credible Attempts
-Reconnaissance

SCM
-FedRAMP ConMon
-Asset Inventory
-SRG/STIG (SCAP)

FedRAMP and ECSB in Parallel



The System Security Plan is the foundation of the assessment. In order to be approved by the FedRAMP PMO as an “in process” CSP, the SSP, along with supporting policies and documents, must be approved.

SSP

The Security Assessment Plan must be created by the 3PAO based on the SSP. The SAP includes key information such as sampling methodology, limitations, tools, and assumptions and must be approved by the Authorizing Official (AO), JAB or Agency

SAP

The Security Assessment Results must be documented in a prescribed template provided by the FedRAMP PMO. Coalfire has extensive experience with providing transparency in the SAR and clearly describing risks in an easy, understandable format.

SAR

The POAM is owned by the CSP with input from the SAR and the 3PAO. Coalfire will work closely with the CSP to identify and recommend risk priorities and mitigation options to meet the requirements of the test objectives.

POAM

PATO

All FedRAMP testing (and only FedRAMP testing) must be uploaded to OMB Max along with the CSP’s reporting requirements.

OMB MAX

Project Management and Coordination with FedRAMP PMO and DISA FSO

SSP Addendum

CSP created an addendum addressing other controls that are above the FedRAMP baseline. This may include additional control requirements, or additional control parameters.

SAP Addendum

Coalfire will created a SAP specifically addressing the unique requirements of the SSP Addendum. This minimizes rework for controls/parameters already included in the FedRAMP assessment.

SAR Addendum

Coalfire will document its assessment results in a SAR addendum, following the format prescribed in the ECSB program.

POAM Addendum

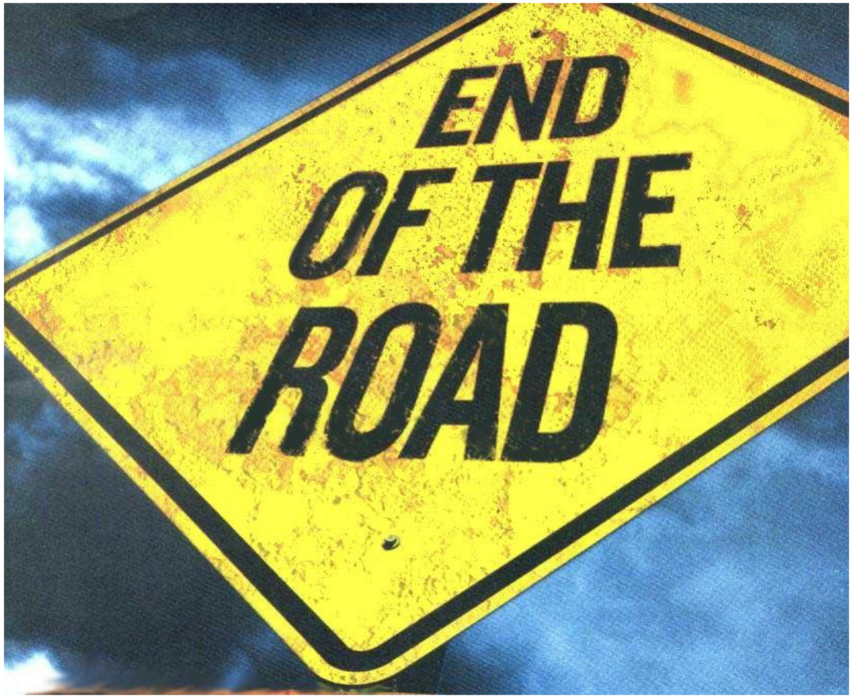
PATO

A separate POAM will be developed that addresses the outstanding items are that above and beyond the FedRAMP requirements and are unique to ECSB controls/parameters.

DISA Portal

The final package will be made available to DISA through an online portal hosted by DISA.

Wrap up



- **Learn**
  - History of FedRAMP
  - Who is in-process?
  - Who is certified?
- **Build**
  - FedRAMP Package
  - Key Challenges
- **Authorize**
  - Program Updates (NIST and FedRAMP)
  - Beyond FedRAMP (DIACAP, ECSB, etc.)
  - What FedRAMP Means for Your Customers
  - Current and Future Models Leveraging an ATO
- **Q&A**

Questions or Suggestions

Send your questions or suggestions to 3pao@Coalfire.com

Visit us at www.coalfirepublicsector.com

Register for FedRAMPcentral using code ISACASF