DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Risk Assessment of Cloud Service Offerings

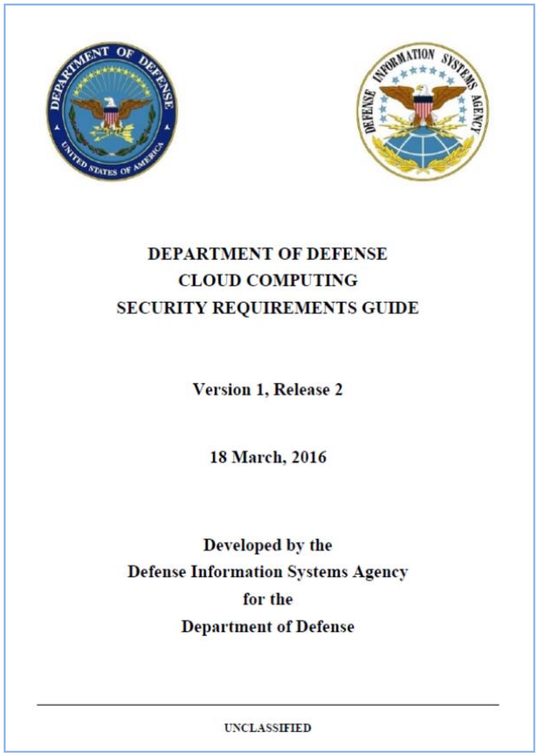
Gordon Bass
Chief, DISA Assessment and Certification Branch (RE52)

22 April 2016

Presentation Disclaimer

"The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government. This brief may also contain references to Unite States Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments."

Cloud Computing SRG v1r2



DEPARTMENT OF DEFENSE
CLOUD COMPUTING
SECURITY REQUIREMENTS GUIDE

Version 1, Release 2

18 March, 2016

Developed by the
Defense Information Systems Agency
for the
Department of Defense

UNCLASSIFIED

Focus of This Brief

Table of Contents

1 Introduction

2 Background

3 Information Security Objectives / Impact Levels

4 Risk Assessment of Cloud Service Offerings

5 Security Requirements

6 Cyber Defense and Incident Response

Information Impact Levels

Level 1: Unclassified Information Approved for Public Release

Level 2: Non-Controlled Unclassified Information

Level 3: Controlled Unclassified Information

Level 4: Controlled Unclassified Information

Export Control, PI, PHI, FOUO and others

Level 5: Controlled Unclassified Information

CUI Requiring Higher Protection, i.e. NSSs

Level 6: Classified Information up to SECRET

Section 3.2 Information Impact Levels

PA & ATO Terminology (1 of 2)

Definitions:

CSP	Cloud Service Provider (vendor)
CSO	Cloud Service Offering (provided by the CSP)
FedRAMP	Federal Risk and Authorization Management Program (authorizes CSOs)
PA	Provisional Authorization (sometimes abbreviated as P-ATO)
JAB	FedRAMP Joint Authorization Board (3 members: CIOs of GSA, DHS and DoD)
3PAO	3rd Party Assessment Organization (independent assessor certified by A2LA.org)
SSP	CSP’s System Security Plan for the CSO
SAP	3PAO’s Security Assessment Plan (including pen-test) for the CSO
SAR	3PAO’s Security Assessment Report of the CSO
DoD PA	DoD Provisional Authorization (granted by DISA AO to the CSP for the CSO)
MO	DoD Mission Owner
AO	Authorizing Official (issues IATT/ATO to MO for the mission system using the CSO)

PA & ATO Terminology (2 of 2)

FedRAMP Provisional Authorization (PA)

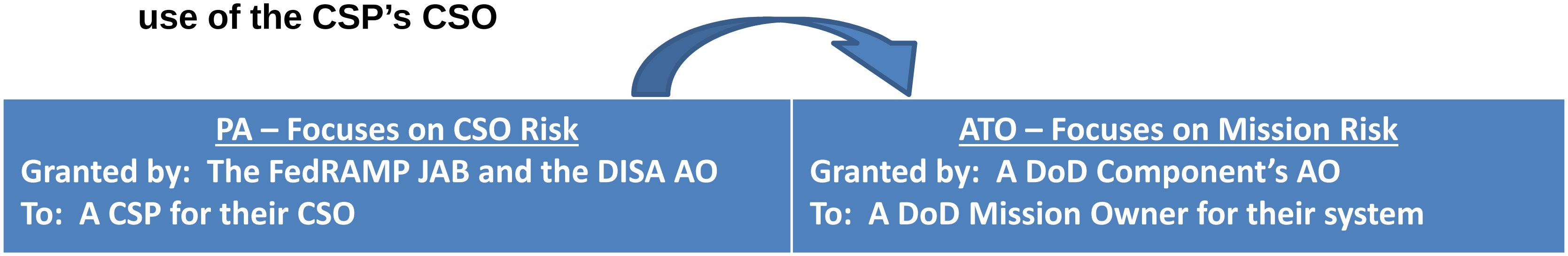
- Issued by the Joint Authorization Board (JAB) to a Cloud Service Provider (CSP) for their Cloud Service Offering (CSO)

DoD PA – Will typically reuse (inherit) a CSP's JAB PA (or Federal Agency ATO)

- Issued by the DISA Authorizing Official (AO) to a CSP for their CSO, based on additional DoD security requirements (Levels 4/5/6)

DoD Authorization to Operate (ATO) – Will leverage a CSP's DoD PA

- Issued by a DoD Component AO to a Mission Owner (MO) for their system that makes use of the CSP's CSO



PA – Focuses on CSO Risk

Granted by: The FedRAMP JAB and the DISA AO

To: A CSP for their CSO

ATO – Focuses on Mission Risk

Granted by: A DoD Component's AO

To: A DoD Mission Owner for their system

Mission Owner AO Tasks (1 of 2)

Mission Owner (MO) Authorizing Official (AO) Tasks:

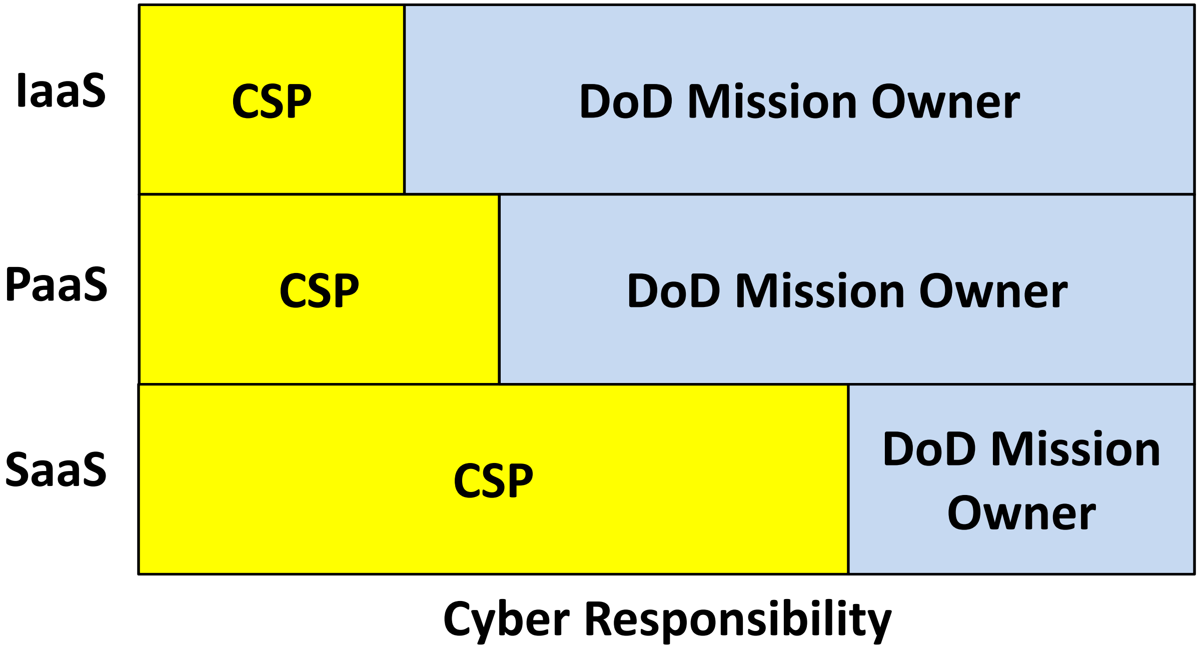
- Identify CSOs with DoD Provisional Authorizations (PAs) that meet mission system data security requirements
- Select the best CSO after comparing risk profiles and other capabilities and characteristics

Mission Owner AO Tasks (2 of 2)

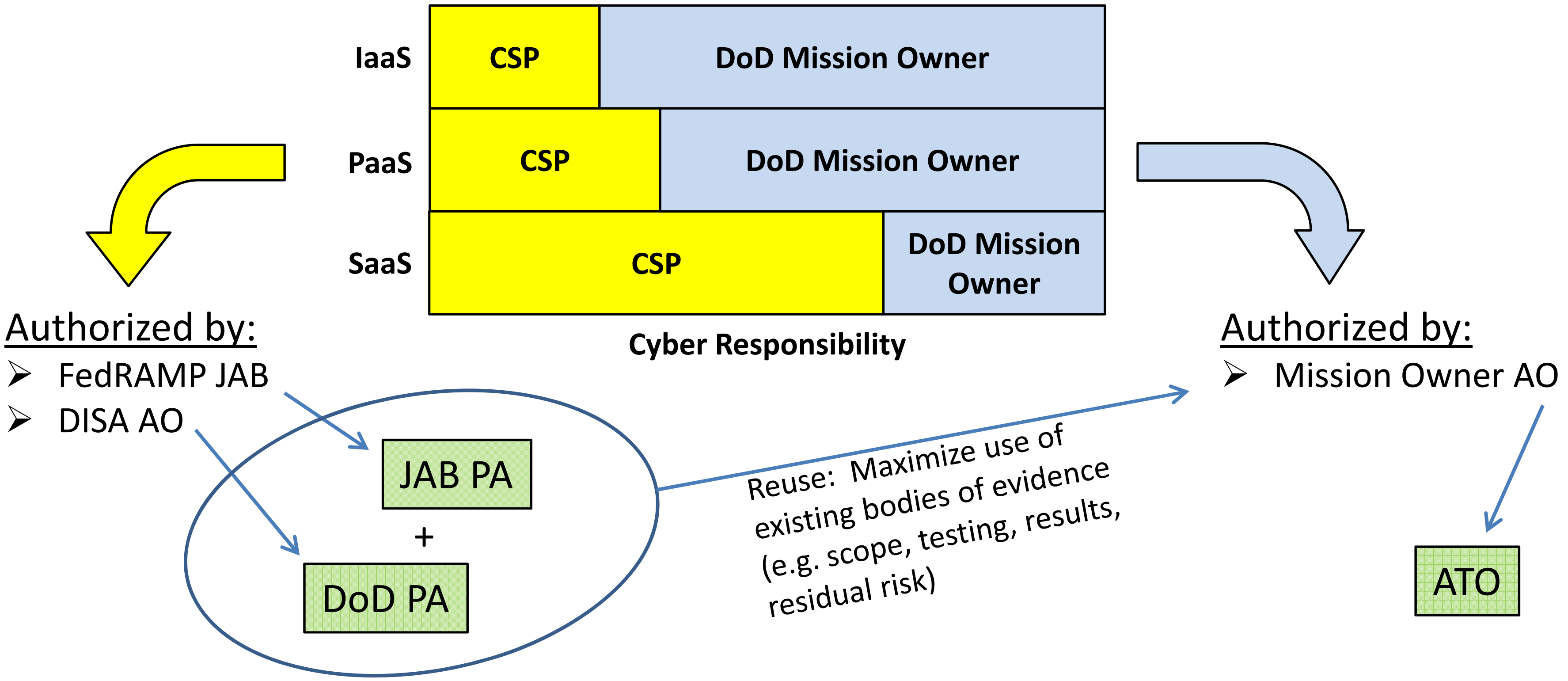
Mission Owner (MO) Authorizing Official (AO) Tasks:

- **Inherit/Leverage – Maximize use of existing body of evidence**
  - Scope of testing adequate? – review 3rd Party's Assessment Organization (3PAO's) Security Assessment Plan (SAP)
  - Test results – review 3PAO's Security Assessment Report (SAR)
  - Residual risk, POA&Ms, continuous monitoring data – review DISA's Certification Recommendation and Provisional Authorization memos
  - Identify and proceed with any additional testing required (with CSP and 3PAO)
- **If risk is acceptable – Issue an IATT/ATO**
  - Accept risk and liabilities identified in the DoD PA, for the MO's unique system and mission
  - Impose any conditions deemed necessary for the secure operation of the CSO, in the context of the MO system requirements, interconnections and data processed

CSP and Mission Owner Cyber Responsibility



Mission Owner AO Risk Decision



IaaS	CSP	DoD Mission Owner
PaaS	CSP	DoD Mission Owner
SaaS	CSP	DoD Mission Owner

Cyber Responsibility

Authorized by:
- ➢ FedRAMP JAB
- ➢ DISA AO

JAB PA

+

DoD PA

Reuse: Maximize use of existing bodies of evidence (e.g. scope, testing, results, residual risk)

Authorized by:
- ➢ Mission Owner AO

ATO

DoD Assessment Process (1 of 2)

Is it really a cloud, or is it an IT service?

- The NIST Definition of Cloud Computing (NIST 800-145)
- Who is the CSP and who is the customer?

CSP:

- Preparation – Create SSP, engage 3PAO to test (SAP) and report (SAR)

DISA/DoD Cloud Team:

- Accept CSP’s assessment package (if complete and ready)
- Validate package (seeking clarification where needed)
- Draft Certification Recommendation
- Brief the Defense Security Accreditation Working Group (DSAWG)

DoD Assessment Process (2 of 2)

DISA AO:

- Issue DoD PA
  - Risk acceptance
  - Identify conditions
  - Memo to CSP
- List in the DISA catalog of DoD PAs

Mission Owner AO:

- Use DoD PA as input to AO decision
- Identify additional requirements and tests if needed
- Issue IATT/ATO – Risk acceptance, identify conditions, memo to Mission Owner (System Owner)

CSP Listings

DoD Compliant CSOs:

- Cloud service offerings with security packages that received a DoD PA

https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx

DoD In-Process CSOs:

- Cloud service offerings actively working with the DoD through the DoD Security Assessment Framework to get a DoD PA

https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Assessment-In-Process.aspx

DISA

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

UNITED IN SERVICE TO OUR NATION