



IaaS BPA Security & Authority to Operate (ATO) Overview

Version 1.0

October 1, 2012



IaaS Awardees, Teaming Partners and ATO

ATO Status as of September 24, 2012

GSA

Vendor	Cloud Storage	Virtual Machines	Web Hosting	Teaming Partner(s)	Date Granted
Apptis, Inc.	ATO	ATO		Amazon Web Services, LLC	Apr 2012
AT&T	ATO	X		No Teaming Arrangement	Jun 2012
Autonomic Resources		ATO		No Teaming Arrangement	Dec 2011
Carahsoft		X		Carpathia Hosting, Inc.	
CGI Federal Inc.		ATO	ATO	No Teaming Arrangement	Oct 2011
Computer Literacy World	X	X	X	XO Communications, Electrosoft, SNS	
Computer Technology Consultants	X	X	X	SoftLayer, Inc.	
Eyak Tech LLC	X	X	X	Horizon Data Center Solutions	
General Dynamics Information Technology		ATO		Carpathia Hosting, Inc.	Sept 2012
Insight Public Sector	X			Microsoft	
Savvis Federal Systems		X	X	No Teaming Arrangement	
Verizon Federal Inc.		ATO		No Teaming Arrangement	Dec 2011

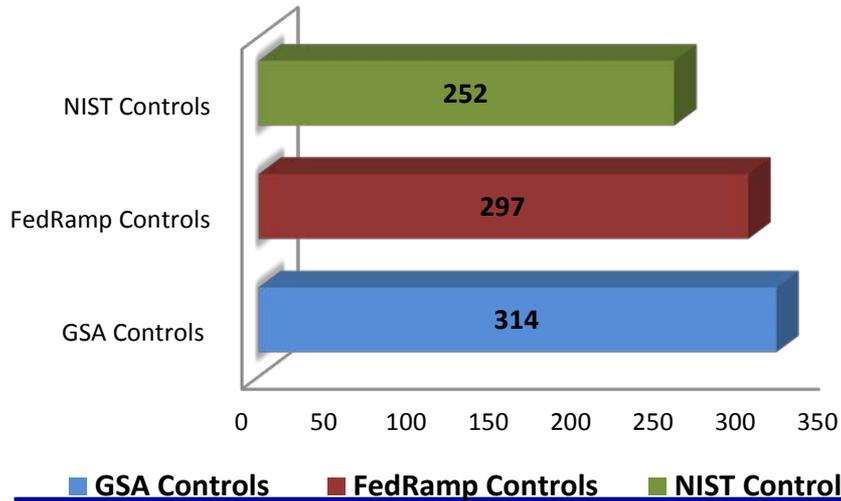
 - Indicates that GSA has granted an Authority-To-Operate



Comparison of GSA IaaS ATO, FedRAMP and NIST baselines



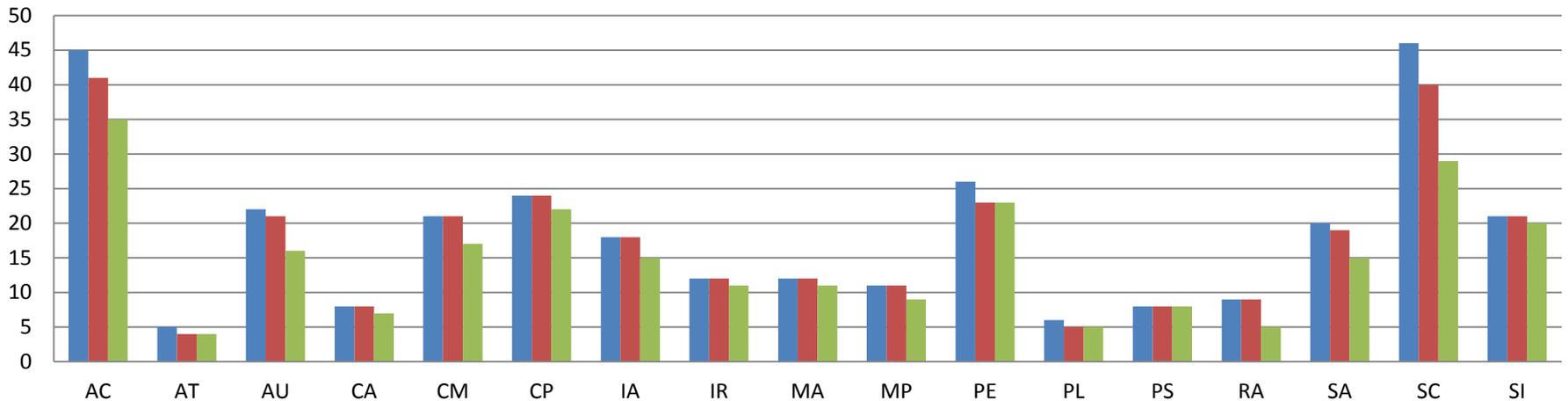
Baseline Security Controls



- The Assessment and Authorization (A&A) processes for IaaS BPA vendors and FedRAMP are similar
- Authorizations achieved through FedRAMP will incorporate the GSA IaaS security controls

~20% of controls will require agency specific implementation/configuration

Security Controls by 17 NIST Defined Families



* Refer Appendix slides for Control families



IaaS ATO FAQs

??????



How GSA IaaS ATO differs from FedRAMP ?

	GSA IaaS ATO	FedRAMP
➤ Security and Privacy Requirements	<ul style="list-style-type: none"> ▪ Based on NIST SP 800-53 r3 ▪ Closely aligned to the to the proposed FedRAMP requirements published November 2, 2010 	<ul style="list-style-type: none"> ▪ Also based on NIST SP 800-53 r3. Requirements updated based on comments received on the published version ▪ Slight differences in security controls for moderate impact levels than GSA IaaS BPA
➤ Desired FIPS 199 impact level	<ul style="list-style-type: none"> ▪ Moderate impact 	<ul style="list-style-type: none"> ▪ Low and Moderate Impact
➤ Independent 3rd party assessor organization (3PAO)	<ul style="list-style-type: none"> ▪ Cloud Service Provider (CSP) chose an assessor which was accepted by GSA 	<ul style="list-style-type: none"> ▪ CSP chooses from FedRAMP accepted list
➤ Authority -To - Operate (ATO)	<ul style="list-style-type: none"> ▪ Granted by GSA FAS/CIO for Government Agencies to leverage 	<ul style="list-style-type: none"> ▪ Provisional Authorization granted by Joint Authorization Board (JAB) consisting of CIO's from DOD, DHS and GSA for Government Agencies to leverage



What is an Authority to Operate (ATO)?

An Authority to Operate (ATO) is a risk-based security decision indicating that a vendor's information system has appropriate safe guards for Government data. An ATO is granted based on the assessment and determination that the management, operational and technical security controls are effectively deployed within the vendor's security boundary.

GSA Infrastructure as a Service (IaaS) Blanket Purchase Agreement (BPA) granted ATO's can be leveraged by any federal agency for the FIPS-199 Moderate Impact Level or lower. This makes acquisitions easier, faster and less costly for agencies to take advantage of the benefits of cloud computing.



Is an Authority to Operate (ATO) required before an order is placed?

Yes, but

- all BPA holders may be solicited,
 - quotes may be received, and
 - a winning vendor may be selected, *contingent upon a GSA issued ATO.*
-

Which vendors have been granted IaaS ATO?

As of September 24, 2012, **six (6)** of the 12 IaaS BPA vendors BPA hold an active GSA issued Authority To Operate (ATO).

The vendors are **Apptis, AT&T, Autonomic Resources, CGI Federal, General Dynamics Information Technology, and Verizon Business**



Should the agency grant an internal ATO on top of the GSA ATO?

The agency procuring cloud services has the ultimate responsibility to review the GSA issued ATO and accept the applicable risks. The GSA issued ATO is for the infrastructure only. The security requirements of an agency may call for additional controls on top of the GSA ATO. The agencies still need to grant an ATO for applications and systems built on top of this infrastructure.

What is the process for an agency to request GSA IaaS ATO documentation?

The agency interested in procuring cloud services may contact the GSA IaaS BPA Manager [Marcelo Olascoaga](#) to request this information.



Guidance for sharing the selected Cloud Service Provider's (CSP) ATO package

1. Due to the sensitive nature of the content included in the CSP vendor's security ATO package, the agency and/or the agency support contractor(s) shall be **allowed to conduct detailed review of the full security package at the GSA or the CSP vendor site location.**
2. The **contractors** contracted for supporting the agency with System Security planning (SSP) activities shall be **under the proper NDA provisions prior to reviewing** this information.
3. **In person presence** of all parties responsible for conducting such a review **required.**
4. Only the three (3) required parts of the CSP vendor's security documentation as listed in the table below shall be provided to the agency for offsite reference

#	DOCUMENT TITLE	DOCUMENT DESCRIPTION
1	Authorization to Operate (ATO) with the Customer Responsibility Matrix (CRM)	The CRM identifies the agency's responsibilities for the contractor's implementation
2	Control Implementation Summary (CIS) from the security authorization package	The CIS identifies the controls and guides the agency to identify and document the controls for their own applications on top of the contractor's infrastructure.
3	Plan of Action and Milestones (POA&M) spreadsheet from the security authorization package	The POA&M identifies the deficiencies and weaknesses in the selected CSP vendor's infrastructure that the agency will inherit.

*** Note:** This guidance is applicable to agencies that have Cloud Service Provider's (CSP) competitors supporting the agency System Security Planning (SSP) and security documentation review process.



When will FedRAMP launch services?

FedRAMP has launched Initial Operational Capability (IOC).

What is the difference between an IaaS ATO and FedRAMP?

The purpose of both programs are the same: to save agencies time and effort in the security process. The Assessment and Authorization (A&A) processes for IaaS BPA vendors and FedRAMP are similar; authorizations achieved through FedRAMP will incorporate the IaaS security controls. FedRAMP Provisional Authorizations will also require the use of a FedRAMP accepted third-party assessment organization (3PAO) and an approval from DoD, DHS and GSA officials who serve on the FedRAMP Joint Authorization Board (JAB).

Do vendors with IaaS ATOs also need to be approved on FedRAMP?

GSA IaaS BPA vendors have been granted an ATO that can be leveraged by other agencies for IT systems and data at the FISMA Moderate Impact Level or lower. IaaS BPA vendors have the option to enter the FedRAMP queue.

For additional information on FedRAMP, visit: www.fedramp.gov



APPENDIX



NIST FAMILIES AND CLASSES

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC