We are ship builders,

not sailors.

Mission Statement

At Autonomic Resources, we provide the FedRAMP authorized cloud security boundaries for all Federal, state, and local government agencies, as well as the private sector, especially critical infrastructure industries such as energy, healthcare, insurance, legal, accounting, and financial.

The Table of Contents

Mutual Non-Disclosure Agreement

Whereas, _____ and Autonomic Resources agree that, in order to facilitate discussions between them relating to potential business opportunities for their mutual benefit, it may be necessary for each Party to disclose certain information on a confidential basis to the other Party. Now, therefore, in consideration of the mutual promises contained herein, each of the Parties hereby agrees as follows:

Confidential Information. In connection with discussions between the Parties, the Parties may find it beneficial to disclose to each other certain nonpublic, confidential, or proprietary information which the Parties desire to protect against unrestricted disclosure or competitive use [hereinafter "Confidential Information"]. Such Confidential Information may include, but is not limited to the following: business and strategic plans, business summaries, business procedures and processes, business and financial forecasts and reports, prospective product offerings, pricing policies and methods, vendor and business partner identities, purchasing methods and information, operational material and manuals, financial data, accounting information and systems, customer lists, customer profiles and purchase preferences, marketing plans, market analysis reports, intellectual property, marketing forecasts, licensing procedures, leasing information, trademarks, service marks, copyrights, patents, proposed trademarks or service marks, trade secrets, technical and engineering data, models, software products, source code, algorithms, object and load modules, content, formulas, design specifications, progress and development reports, coding sheets, flowcharts, employee information, corporate information, and phone lists.

Both Parties agree to keep in confidence all Confidential Information received, and not distribute, disclose, or disseminate such Confidential Information in any way to anyone except to the minimum number of employees or consultants of the receiving Party with a need to know and who are involved in a consideration or evaluation of the Confidential Information; *provided however,* that such employees or consultants have been advised of the obligations to protect the Confidential Information, and *provided further,* that notwithstanding the foregoing, the receiving Party shall be liable for any misuse of such Confidential Information by such employees or consultants.

No Commitment. It is understood that this Agreement does not obligate either of the Parties to enter into further business discussions. Each Party acknowledges that Confidential Information provided by the disclosing Party does not, and is not intended to represent a commitment to enter into a business relationship with the receiving Party.

No License. Nothing contained in this Agreement shall be construed as granting or conferring any rights by license or otherwise in any Confidential Information disclosed by the Parties.

Governing Law. This Agreement shall be governed by and construed in accordance with the internal laws of the State of New York and not the principles of conflicts of law thereof.

In witness whereof, the Parties have caused this Mutual Nondisclosure Agreement to be executed by their duly authorized representative as of this date, September 30, 2014.

_____ _____

Thomas Thomson, Autonomic Resources Representative

A. Letter of Introduction

“The only truly secure system is one that is powered off, cast in a block of concrete, and sealed in a lead-lined room with armed guards.” – Professor Gene Spafford, Purdue University

“Our core objective is to develop secure cloud solutions that facilitate the specific needs of Federal agencies based on FedRAMP and DISA protocol and certifications.” - John Keese, Founding Partner

As managing partner of Autonomic Resources, I would like to present for your investment consideration our incredible Federal Cloud Service Provider opportunity. Over the past four years, we have dedicated our efforts to building the most resourceful solutions to facilitate the Federal Government’s Cloud First Initiative. What we have accomplished on a limited budget is unprecedented. What follows is the remarkable result of our tenacity, dedication, frugality, and ingenuity. Our story begins with the emergence of cloud computing.

What is cloud computing?

Cloud technologies have transformed the way computing power is bought, sold, and delivered. Rather than purchasing licenses or hardware, users may now obtain computing power as a service by buying only as much as they need, and only when they need it. Additionally, cloud computing allows a focus on mission-enabling capabilities, rather than maintenance of legacy infrastructures.

This new business model delivers vast efficiency and cost advantages that have not been lost on the Federal Government. The enormous potential of cloud computing has prompted the United States Federal Government to look to the cloud as a means of IT infrastructure reorganization and IT budget realignment.

In December 2010, the Office of Management and Budget [OMB] issued a Cloud First Strategy for Federal Government computing needs. Under this policy, government agencies are compelled to use cloud computing resources rather than expensive government-owned and operated data centers to boost computer operations. This federally mandated strategy required that each agency Chief Information Officer [CIO] fully migrate defined services to a cloud solution by June 2014, and define a roadmap for the implementation of cloud-based solutions moving forward.

Accordingly, a new ecosystem is being developed for cloud service providers in the Federal space. This new ecosystem will contractually determine access to the massive untapped Global Government Cloud Market over the next decade. Our objective is to deliver the most versatile and cost-effective set of solutions in this new FedCloud Ecosystem.

What is FedRAMP?

The sensitive nature of the Federal Government’s computing systems and electronic data demands the highest levels of comprehensive security. In order to mitigate potential security and control risks, the Federal Risk and Authorization Management Program [FedRAMP] was created to oversee all of the FedCloud offerings. Through the use of a thorough accreditation process, FedRAMP ensures that cloud service providers [CSPs] stay within the important security boundaries as defined by NIST [National Institute of Standards and Technology] and as dictated by government agencies.

The most notable achievement of our remarkable pursuit is our list of government security accreditations. Autonomic Resources, operator of the Autonomic Resources Cloud Platform [ARC-P™], is the only platform fully accredited by the FedRAMP JAB [Joint AUthorization Board] and Defense Information Systems Agency [DISA] certified-secure CSP for the United States Federal Government and all of its associated agencies and operations. As a result of this unique certification situation, we hold unprecedented and unrivaled access to the rapidly expanding Federal Cloud Ecosystem. ARC-P is the preeminent cloud solution created for the Federal Government.

What is ARC-P?

ARC-P™ is our Infrastructure as a Service [IaaS] offering, and it effectively supplies our government clients with raw computing, storage, and networking power. ARC-P provides an elegant, fully patched, and compliant hosting environment designed to run a variety of application software. Our expertise in open source technologies allows us to deliver the most lightweight and reliable application architecture to the Federal Government. The numerous advantages of open source have made it the gold standard for Federal Government Cloud Computing.

ARC-P supplies the desired elastic computing power, storage, supporting infrastructure, and accelerated application deployment that can be acquired and exploited on demand. Our government clients can now rapidly utilize certified-secure data center capabilities without the extensive cost and administrative work associated with purchasing and maintaining data center facilities and associated computing infrastructure.

While Autonomic Resources has the capability to produce competitive cloud service offerings, we feel that our intrinsic value is further enhanced by the desire of other CSPs to acquire similar government accreditation. We intend to leverage our prime position and close relationship with FedRAMP to provide first-mover advantage to other CSPs, systems integrators and software providers in the acquisition of a FedRAMP Authority to Operate [ATO]. As the first CSP to be accredited by both the FedRAMP JAB and DISA, every software solution provider, data center operator, and systems integrator desiring access to the lucrative Federal Cloud Ecosystem can be confident in our ability to deliver.

In short, we are not simply a cloud service provider - we are a world-class start-up creating unique value for accelerated access to the revolutionary new Federal Cloud Ecosystem. We invite you to join us on this journey.

Sincerely,

Tom Thomson
Managing Partner

B. Why we are the FedCloud Market Leader

"Everything is moving to the cloud, and we provide secure access to the Federal Cloud better than anyone else in the world. The amazing array of technologies that we are working on in the ARC Oven outperform anything else in the Federal Cloud access realm." - John Keese, Founding Partner

The total addressable Federal Cloud Market is the most significant new opportunity in the rapidly evolving cloud ecosystem, and it remains an unresolved market [URM]. Not only do we provide the essential FedRAMP and DISA security accreditations that allow access to this narrowly restricted market, but we also act as a driving force in the creation of the technology stacks that are essential to the emerging Federal Cloud Ecosystem.

Here is how we have emerged as the FedCloud Market Leader:

- ➔ **First-mover access to the emerging Federal Cloud Spend.**
  As the first-mover in this space, we provide an opportunity for first-in positioning in all of the desired categories of cloud platforms and services. No other CSP is so uniquely positioned to bring cloud-enabling technologies to the center of this transformation.

  The secure platforms and service offerings we are building and certifying give our FedCloud Ecosystem partners the opportunity to dominate the developing cloud supply chain. Our first-mover capability allows us to stake out a long term position of dominance within this new FedCloud Ecosystem. And, just as remarkably, we are poised to stake out a long term position of dominance in the commercial market with the inevitable migration of FedRAMP security boundaries to the critical infrastructure industries such as energy, healthcare, insurance, legal, accounting, and financial.

- ➔ **FedRAMP Certified Physical Facilities.**
  At Autonomic Resources, we have taken a leadership position in working with FedRAMP to include our fully certified secure data centers as part of the essential FedRAMP IaaS security boundaries.

  Our secure data centers are both FedRAMP and DISA certified, allowing us to provide a wide array of fully accredited data center solutions to the Department of Defense. Our secure data centers are available as managed colocation facilities, giving us the unique ability to assist government agencies with their migration to the cloud.

- ➔ **Accelerated Application Deployment.**
  Our ARC-WRX trusted PaaS cartridges and container technologies provide the environments necessary to accelerate the building, certification, and deployment of secure Federal Cloud applications. We expect to complete the ARC-WRX PaaS FedRAMP JAB accreditation process by November, 2014.

➔ **Lead Resource in Award Capture.**
Our innate understanding of this unresolved market [URM] makes us a coveted teaming partner for a wide range of cloud companies, including hardware and software technology partners, SaaS providers, and large government systems integrators.

Today's government procurements have been transformed from component, time, and labor based acquisitions to consumption-based contracts. No Federal CSP shares Autonomic Resources' ability to effectively assist teaming partners in the pursuit of these consumption-based contracts.

C. Our Three Key Divisions

Initially, our mission at Autonomic Resources was simply to conceptualize, design, build, and accredit secure cloud solutions to facilitate the specific needs of Federal agencies through certifications based on the stringent Federal Risk and Authorization Management Program [FedRAMP] and Defense Information Systems Agency [DISA] standards. And while we certainly hit our mark on this objective, we have used our FedRAMP ATO as the foundation for our ever-expanding role in the entire cloud ecosystem.

Today, our ARC Oven has provided us with the unprecedented and remarkable capability to provide the FedRAMP Cloud Security boundaries for all Federal, state, and local government agencies, as well as the private sector - especially critical infrastructure industries such as energy, healthcare, insurance, legal, accounting, and financial.

We have separated our unique and unprecedented Cloud Security activity into three key divisions: **The ARC Oven, FedCloud Express, and FedCloud Secure.**

The ARC Oven

The Autonomic Resources Cloud [ARC] Oven is our defining asset. It is, fundamentally, our research and development division which focuses on product development, accreditation, and launch.

> **"We are the Federal Cloud Ecosystem's leading R&D company, and we have every intention of extending and maximizing our leadership position."** - John Keese, Founding Partner

At Autonomic Resources, we utilize the ARC Oven to identify, develop, accredit, and launch trusted cloud computing products and platforms for Federal government agencies and contractors. In addition to providing us with the intellectual property crucial to our operation, the ARC Oven provides licenses and exclusivity agreements to various strategic, teaming, and corporate partners.

The ARC Oven is recognized in the Federal Cloud Ecosystem for our superior set of certified-secure cloud offerings. We have been awarded a FedRAMP Provisional Authority to Operate [ATO] as well as an ATO at Impact Levels 1 and 2 from DISA for both our government community and private IaaS offerings. The superior value of our ARC Oven is continuously validated through the on-going delivery of innovative FedRAMP and DISA certified-secure cloud platforms and services.

As the primary generator of our coveted intellectual property, the ARC Oven sets us apart from other CSPs through our responsiveness to emerging Federal Cloud requirements, as well as by our thoughtful architecture implementation of open standards. Our ARC Oven process is the only product launch capability developed with FedRAMP accreditation as the fundamental guidepost for all its cloud activities.

The ARC Oven has three main activities:

- **FedRAMP ATO**
  Our ARC Oven develops, maintains, and enhances our Autonomic Resources Cloud Platform [ARC-P] which provides our critical FedRAMP IaaS Authority to Operate [ATO], as well as the Department of Defense's DISA certification [and all other necessary authorizations and certifications].

  Our FedRAMP JAB Provisional ATO is for the most stringent form of FedRAMP accreditation based on NIST and FISMA standards. This comprehensive ATO facilitates all Federal Cloud teaming pursuits, and it is the foundation for all accredited security activity in the Federal Cloud. All enhanced capabilities refer back to this baseline, making us the leading and most agile Federal Cloud Service Provider for all teaming pursuits and agency specific requests.

- **Cloud Compute**
  Our ARC Oven provides the actual cloud compute in our FedRAMP Authorized Secure Data Centers for all of our licensed partners.

  It is important to note that the FedRAMP security boundaries include the secure data centers where the ongoing compute activity resides. The FedRAMP continuous monitoring requirements for security boundaries are often confused as a firewall with intrusion detection type security presence - rather than a secure environment including the physical location, configuration management, access controls, and disaster recovery policies which must also meet the stringent security standards demanded for a FedRAMP ATO.

  Once a cloud solution is established as an authorized resource in our secure environment - it is unlikely to be re-engineered or moved - making our cloud offering very "sticky." This makes our ARC Oven an extremely enduring long term resource for recurring revenue.

- **Licensing Agreements**
  Our ARC Oven division develops, negotiates, and maintains the licensing agreements with all of our various Federal Cloud Ecosystem partners, as well as all of the authorization and certification licensing agreements with our associated FedCloud Resources.

  The ARC Oven division also promotes exclusive licensing arrangements with strategic suppliers and teaming partners through our Medallion and ARC-PE exclusivity and preferred supplier programs.

FedCloud Express

At FedCloud Express, we are the only cloud service provider offering an accelerated, secure, and agile accreditation consulting process for the Federal Cloud, and that is exactly what the Federal Cloud Initiative mandates.

Whether a cloud solution provider requires their Software as a Solution [SaaS] services to be FedRAMP accredited [in order to make their services available to Federal agencies], or a Federal agency requires a

specific SaaS to be FedRAMP accredited, our FedCloud Express resource is there to facilitate and accelerate the actual FedRAMP authorization process for all of our clients.

FedCloud Express provides the re-platforming and the knitting together of new architecture for companies that require a FedRAMP ATO for their SaaS services. Once we successfully take a SaaS through the FedRAMP process, we continue to generate revenue from the consumption of our cloud services through our application partner's SaaS compute activity in our cloud. And, once we are established as their CSP, clients become reliant on us for ongoing FedRAMP compliance services like managed support services and continuous FedRAMP security monitoring.

FedCloud Express provides four unique venues for FedRAMP authorization [all Powered by ARC-P].

- ➔ **FedRAMP Joint Authorization Board [JAB]**
  FedCloud Express offers an accelerated path to authorization through the JAB process. The FedRAMP Joint Authorization Board [JAB] approves eligible cloud solutions for processing and evaluation. This is the desired route for SaaS FedRAMP authorization. ARC-P was the first to receive the FedRAMP Authority to Operate through this process, and we are clearly the leader in this category.

- ➔ **Federal Agency Sponsorship**
  Because the Joint Authorization Board is backlogged, FedRAMP now allows Federal agencies to take desired cloud solutions through the FedRAMP certification process independent of the FedRAMP JAB. Agencies can now leverage the FedRAMP PMO process and the JAB-approved FedRAMP security authorization requirements and tools as a baseline when initiating, reviewing, granting and revoking security authorizations for cloud services.

  At FedCloud Express, we are uniquely positioned to provide these Federal agencies [and their sponsored SaaS providers] with the efficacy necessary to successfully navigate the accreditation process. Currently, we are the only viable resource for agencies to utilize for this accelerated process that leverages control inheritance across our existing accredited platforms, and it is all powered by ARC-P.

- ➔ **Teaming Partner Pursuits [Lead Resource in Award Capture]**
  With FedCloud Express, we provide consultative cloud engineering and proposal response consulting for Federal Award Pursuits. Our deep involvement with FedRAMP and DISA as the only independent service oriented CSP provides us with a framework for the creation of successful award pursuits in the new Federal Cloud Ecosystem [Amazon provides AWS pricing packages to multiple systems integration partners and provides no support or ongoing services]. Our work includes making the SaaS work in the ARC-P cloud and packaging it for FedRAMP.

  As a key teaming partner, we are engaged to assist in systems architecture and design in order to guide our partners through the FedRAMP process for the award pursuit. Once we secure a Federal Award, we generate revenue from the consumption of our cloud services through direct task orders that must utilize our cloud [as per our teaming agreement].

- ➔ **FedCloud Express App Builder [ARC-WRX]**
  Our FedRAMP Authorized ARC-WRX accelerated application deployment program facilitates both the buildout of specific Federal agency desired SaaS solutions as well as the eventual creation of a FedRAMP Certified App Store operating within our FedRAMP security boundaries.

  Our ARC-WRX PaaS trusted cartridges provide the environment to accelerate the building, certification, and deployment of secure Federal cloud applications. Product built in ARC-WRX is immediately ready for 3PAO and Federal Agency specific certification.

  In addition to our FedRAMP Certified IaaS, our new FedRAMP Certified PaaS Platform [ARC-WRX] facilitates an accelerated build out for certifying desired SaaS solutions, advancing our well-earned reputation as the most responsive FedRAMP Cloud Service Provider.

  Our forthcoming app store marketplace platform will handle complex billing relationships between users, service levels, billing intervals, free trials, one-time fees, introductory pricing, upgrades, and renewals. Additionally, the platform will empower customers to manage their own subscriptions and provision users on demand within their own cloud environments. FedCloud Express fully intends to provide the app store for the entire FedCloud Ecosystem, thereby disrupting and transforming the entire Federal Cloud supply chain.

FedCloud Secure

In addition to providing accelerated authorization for our clients through FedCloud Express, Autonomic Resources also provides the necessary and continuing services demanded by FedRAMP authorized activity through our FedCloud Secure division.

FedCloud Secure also provides the FedRAMP cloud security boundaries and consulting services for the private sector, especially critical infrastructure industries such as energy, healthcare, insurance, legal, accounting, and financial.

- **Security Consulting Services**
  Our FedCloud Secure Security Consulting practice offers a wealth of experience across a variety of today's top security challenges. Our certified consultants represent some of the top talent in the industry, and we pride ourselves on our ability to tackle security challenges of any size for Federal Agencies and Federal Government software suppliers.

  We have the experience necessary to assist agencies and SaaS providers in the management of the comprehensive Federal Information Security Management Act [FISMA] and associated NIST-800 controls. We are also uniquely positioned to assist SaaS providers and agencies with the FedRAMP Security Package.

- **Cloud Service Provider [CSP] Services**
  In essence, cloud computing delivers common ground among application developers, telecommunication providers, and hardware-software providers. This translates into a significant set of business requirements including: high-performance networks; strong customer relationships; application delivery expertise; the continual infusion of innovation; customer self-service functionality; future customer needs predictions; and integrated Operations Support Systems and Business Support Systems.

  Autonomic Resources' FedCloud Secure CSP consulting services provide our Federal Cloud customers with the expertise they need to plan, transition, implement, and manage systems in the new cloud-integrated computing world.

- **Real Time Compliance and Risk Management**
  FedCloud Secure has established FedRAMP authorized measures, metrics, status monitoring, and control assessment frequencies that alert users to changes in information system infrastructure and environments of operation. The system reports the status of security control effectiveness in a manner that supports continued operation within acceptable risk tolerances.

  Our Continuous Monitoring as a Service [CMaaS] program collects the data required for the defined measures and features automated collection, analysis, and report generation. Our software analyzes the report results and provides remediation strategies based on test outcomes.

  This continuous monitoring approach extends to clients and software providers operating in our ARC-P cloud, assuring the highest levels of security as required by FedRAMP and DISA. Our continuous monitoring approach makes security and accreditations real and on-going.

All of our FedCloud Secure services are becoming increasingly necessary [and desired] in the commercial market. We are prepared to facilitate any American based and owned company.

D. Strategic Investment Opportunities

Through this offering, it is our intention to demonstrate our extraordinary value to knowledgeable strategic investors based on our ARC Oven, FedCloud Express, and FedCloud Secure resources. Not only are we positioned at the center of this Federal Cloud revolution, but we have created the authorized platforms and reference architectures that will be used as the standard for the entire FedCloud Ecosystem for the foreseeable future. Now is the time for us to take the full measure of our competitive advantage in the marketplace.

Investor Profile
We are looking forward to working with investors who truly understand our competitive advantage and can help us grow it to maximize our full potential. We are seeking an investor that can provide potential liquidity to the owners, while offering additional financial and strategic resources to assist us in leveraging our powerful market position to drive growth down multiple channels.

We would also consider a strategic partner interested in fully absorbing Autonomic Resources.

Strategic Investor
With our combination of almost limitless scale, ready-to-be-activated profitability, top-tier Federal government access, breadth of services, and talented professionals - Autonomic Resources presents a compelling investment or acquisition opportunity for a strategic investor looking to enter [or maximize their current access to] the Federal Cloud Ecosystem.

We have several pathways that can be leveraged for growth, including expansion of existing business, growth in nascent practice areas, and capitalizing on new opportunities in strategic industries in the commercial space that will imminently fall under Federal cybersecurity scrutiny. Our certifications, reputation, and strategic positioning among our client base, key teaming partners, and Federal agencies is unparalleled - positioning us at the epicenter of the new Federal Cloud Ecosystem.

Equity Investor
Although our primary focus is an alliance with a strategic investor who will accelerate and optimize our unique access to the enormous Federal Cloud Market, we will consider an equity investor who will provide us with the funding to develop the necessary resources independently.

Equity Investment
For investors looking for full equity involvement, the partnership is not looking to cash out any of the investment. All monies invested will remain in the company. The monies will be utilized to satisfy current debt and facilitate the fruition of our FedCloud Express and FedCloud Secure swim lanes.

E. Our 8 Key Competitive Advantages

As the pioneering architects of the FedCloud EcoSystem, we have clearly established a number of competitive advantages. Our FedRAMP and DISA certifications mean that we have unparalleled security protocols that can be utilized for all types of sensitive government cloud applications. No other Cloud Service Provider [CSP] has the same cloud security capabilities as Autonomic Resources.

1. **Dramatically Reducing Client Costs**
Autonomic Resources Cloud Platform [ARC-P] eliminates the up-front hardware investment, so Federal agencies can focus their IT resources on rapid application deployment. ARC-P enables our clients to scale up or down to handle changes in computing requirements, reducing the need to forecast traffic. This is the essence of the anticipated cloud compute value, and no one provides more value than our ARC-P.

2. **First to FedCloud Authorization**
We have established our competitive advantage in the Federal Cloud by repeatedly being first. Our Iaas offerings were first to FedRAMP and first to DISA ATO, beating competitors like Amazon AWS, IBM, Lockheed Martin, HP, and Microsoft.

Not only were we first, we beat our cost of entry projections by 40%. While an estimated half a billion dollars has been spent by over 100 companies attempting to secure FedRAMP ATO's, we were able to successfully acquire an impressive array of certifications and ATO's for only $8.5M to date. We were are currently over 40% below our initial projection of $15M cost of entry, and well below the $23M and $40M allegedly spent by CGI and VMWARE respectively.

3. **Open Source**
John Keese's is a long time champion of the Open Source movement, with a unique focus on open source for government. Our open source approach has proven to be the most innovative, effective, and efficient foundation for the development of the FedCloud architecture. Open source is the best choice because it enables a best of breed solution and avoids the preference angle. Open source is inherently free of conflict and it is the most innovative option out there for time to market, scale, and technical depth.

We have effectively put open source software at the forefront of the certification race, and we are not alone in recognizing its value. The Federal Government has long understood the benefits of open source software which utilizes open standards-based components which help to ensure application portability while eliminating vendor lock-in. All of the ARC Oven products are based on the open source solutions that are fundamental to Federal contract acquisition.

No other company has fully embraced such an advocacy of the government's Cloud First, Open Government, and Data Center Consolidation directives. The ARC Oven continues to deliver computing platforms and software products that earn both FedRAMP and DISA ATOs, cementing our position as a leader in the delivery of accredited cloud products to Federal customers.

4. **Built Specifically for the FedCloud**
The core strength of Autonomic Resources is our ability to identify emerging Federal cloud computing market trends and to define research and development efforts to build platforms and offerings to specifically address those requirements. This is coupled with our unique ability to certify and launch those offerings under the stringent standards set forth by government oversight bodies.

No other company approached the Federal government's Cloud First Policy in this fashion. No other company was built specifically to secure this position in the Federal Cloud ecosystem, nor can they offer the sustainable capability to continuously launch new offerings.

"We are at the epicenter of the Federal Cloud Ecosystem." - John Keese, Founding Partner

We have made a deliberate and focused decision to invest in building this unique position and specific capability. While some may categorize this approach as "non-revenue building," we are certain that establishing this capability at the initial stages of the FedCloud computing wave has established us with a first mover advantage and market position that is sustainable for the long-term.

While our competitors struggle to achieve baseline FedRAMP accreditations, we keep stretching our recognized lead by extending the ecosystem with new accredited platforms and software products produced by the ARC Oven - and that is exactly where we have built our remarkable and sustainable value.

5. **Primary Contract Position and Capabilities**
Our investment over the past four years has focused solely on our ARC Oven research and development initiatives to create our unique position in the Federal Cloud, and it has resulted in an unmatched position in this

emerging cloud compute and distribution space. We have coveted contract vehicles at our disposal, as well as key relationships throughout government agencies in all branches that recognize Autonomic Resources as the leader in the government community Cloud.

Our government-focused business development and contract pursuit team has unparalleled experience in the contract acquisition process and we are uniquely qualified in the area of Cloud-based contracts. Our position is also enhanced by the fact that the GSA Cloud awards are under cooperative procurement agreements with all state and local government entities. This market remains largely unaddressed by the traditional contractor and vendor community.

6. **Desired Managed Services**

Autonomic Resources is also a leader in the deployment of the managed service models that are taking shape around Cloud computing platforms and software offerings. Traditional information technology contracts, based on system counts, are being replaced with cutting-edge cloud deployment models.

Cloud deployment models propelled by initiatives such as the Federal Data Center Consolidation Initiative [FDCCI] will continue to assist in Cloud growth, reducing on-site labor contract revenues. The shift toward a Cloud "devops" model will only accelerate blurring of the lines between software development, infrastructure deployment, and management that the traditional system integrator has depended on to drive revenue streams. As development activities are driven to the Cloud, application development services will follow suit. Autonomic Resources is positioned to enable traditional technology and services suppliers to reshape their offerings under these new models.

7. **Commercial Extension**

As pending cybersecurity legislation extends FedRAMP-like cloud compliance standards to industries deemed critical infrastructure [energy, health care, insurance, legal, accounting, and financial], we anticipate great demand for the high security cloud products and security monitoring platforms delivered by the ARC Oven. We have consistently demonstrated our ability to meet the stringent FedRAMP and DISA standards, and we believe this leaves us well equipped to handle such commercial demand.

8. **Ascendant Technical Expertise**

Our technical expertise has positioned us as the vanguard of the new FedCloud Ecosystem. Driven by the vision and leadership of John Keese, our proactive approach with the Federal Government's Cloud First Mandate has allowed us to be first-to-market with new certified-secure cloud computing products.

Our FedRAMP knowledge and experience is unmatched in the FedCloud Ecosystem, and we credit our success to our focused business model which includes our ascendant technical expertise and adroit application of partnership resources. Here's how we do it:

- ➔ **Customer Centric Innovation**
  The basis of our continuous innovation is the ever-increasing needs and demands of the FedCloud Ecosystem. We are driven by the defined mandates of the Federal government's cloud computing initiatives and the requirements defined by specific agency RFP requirements. Our FedCloud Express team takes a customized consultative approach to providing value-added solutions, with the goal of ensuring a successful and efficient outcome for our government clients.

- ➔ **Methods and Tools**
  Autonomic Resources has developed a number of proprietary tools and processes to ensure rapid and scalable delivery of accredited trusted cloud solutions. As clients continue to rely on Autonomic Resources for support, our relationship base, contractual assets, and unique position in the FedCloud Ecosystem has continued to grow.

- ➔ **Specialized Knowledge**
  Our research and development team at Autonomic Resources is widely recognized for our expertise. In particular, our development staff is widely recognized as the leader in the promotion and adoption of open source technologies and in developing and deploying next generation cloud based computing architectures and platforms.

  With regard to security, our staff has led the market in the development and accreditation of security packaging and continuous monitoring. We also possess unique skills and knowledge in the areas of cloud pricing, contract pursuit, and contract response modelling and coordination.

- ➔ **Flexible & Responsive Business Model**
  Our agile approach to the identification of new cloud opportunities allows us to continually innovate and stay ahead of the competition in the delivery of certified products, new approaches, new product, and

new company spin-offs. Daily review sessions are used both as checkpoints to current work processes and deliverables and as idea generators for new product development.

➔ **Nurturing Partner Relationships**
Our investment partner strategy delivers true transformational computing resources in order to perpetuate the open cloud strategy.

Our partner ecosystem has been developed from all segments coalescing around the cloud. We have included the industry leading systems integrators, hardware and software manufacturers, telecommunications, and data center providers [all of whom are using this symbiotic relationship to gain accelerated authorized access to the burgeoning FedCloud EcoSystem and its anticipated spend].

F. Monetizing the FedCloud Market

Autonomic Resources' business development strategy has maintained an effective, rewarding, and specific focus on our remarkable FedCloud Ecosystem buildout [including market creation, product development, accreditation, and launch activities through the ARC Oven]. While we intend to continue to direct and invest in our highly sought-after ARC Oven resource in this way, we have established 4 exclusive and valuable revenue swimlanes for future investor and partner deployment.

1. **Teaming Award Pursuits**
As the shift to cloud-based contracts continues to increase, teaming partners are increasingly calling on FedCloud Express to facilitate and coordinate their lucrative pursuits based on our accreditations, our unique understanding of the changes in the procurement process, and our facilitative engagement process.

FedCloud Express provides the consulting and engineering services as the key facilitator of Federal government cloud contract pursuits. Our process includes storyboarding solution approaches, architecting platforms, integrating software into demonstrable proofs-of-concept [POC] in the ARC-P cloud, developing pricing structures, as well packaging solutions for FedRAMP processing and accreditation.

Revenue in this category is generated through proposal preparation, systems integration, and guidance through the FedRAMP accreditation process.

2. **FedRAMP Accelerated Authorization**
We provide the re-platforming and the knitting together of new architecture for companies that simply want a FedRAMP ATO for their SaaS services. This activity is similar to the Teaming Award Pursuit activity but is shorter in term by nature, and focuses on technical migration and FedRAMP accreditation for SaaS partner existing software applications.

Our work includes re-architecting platforms, software integration the ARC-P cloud, and packaging solutions for FedRAMP accreditation.

Revenue in this category is generated via proposal preparation, systems integration, and guidance through the FedRAMP process.

3. **Consumption of Cloud Services**
As agency customers, software providers serving agencies, systems integrators, and storage customers move their applications and data to the ARC-P cloud, revenue is earned for the basic consumption of the software, storage, and compute resources in the ARC-P cloud.

Our high margin pricing is based on virtual machine and storage units per hour, week, or month and can vary widely depending on the scope of the deployment.

4. **The ARC-PE Program**
The ARC-PE program is designed to provide our technology partners exclusive or preferred supplier access to new Federal government cloud compute spending. It also can provide them with protection for their existing Federal IT market position [as cloud spending disrupts the traditional sales channel]. With an investment in the

ARC-PE program, our partners are guaranteed exclusivity or preferred status as a supplier to ARC-P cloud technologies for agreed upon platforms and periods of time.

- ➔ **Systems Integrator Pursuit Exclusivity**
  Autonomic Resources offers select systems integration teaming partners the opportunity to secure an exclusive partnership for specific Federal contract pursuits or on an agency-wide basis.

- ➔ **Technology Supplier Exclusivity**
  The ARC-PE Technology Supplier program is designed to provide our technology partners exclusive or preferred supplier access to new Federal government cloud computing spending. This program acts as protection for their existing Federal IT market position and market share as cloud spending disrupts the traditional sales channel.

  With an investment in the ARC-PE program, our partner is guaranteed exclusivity or preferred status as a supplier to ARC-P cloud technologies for agreed upon platforms and periods of time.

G. The Competition

Although cloud adoption is rapidly accelerating, traditional internal IT department culture and embedded legacy systems architectures remain the most significant challenge to broad and rapid adoption of the cloud. These legacy systems, and personnel [contractor supplied and direct government employees] are generally slow to adapt to new technology platforms.

At Autonomic Resources, we continuously focus on providing education and awareness for end customer agencies, teaming partners, and hardware-software manufacturers to promote the opportunities and benefits associated with elastic, asset-free computing.

As cloud adoption accelerates, our unique set of accreditations and intellectual property sets us apart from our competitors. While surprisingly few of our competitors possess vaguely similar accreditations or product offerings, none have Autonomic Resources' competitive edge. It has become apparent that it has turned into a two horse race: Amazon AWS vs Autonomic Resources.

Autonomic Resources is recognized by customers and partners in the Federal Cloud space for creating a superior set of offerings and for the assistance we provide in building platforms, while delivering deft guidance throughout the arduous accreditation and launch process. This assistance is critical and has challenged our larger competitors.

Besides Amazon, various other competitors are promoting cobbled together "cloud" offerings based on heavy architecture legacy product sets and overpriced me-too virtualization platforms. The large Systems Integrator [SI] deployments are typically custom built to facilitate defensive contract maintenance strategies rather than promotion of the true utility based computing desired by the Federal government. Only ARC-P has built upon hardened open source architectures to deliver a cost effective and elastic cloud offering deemed as secure by the FedRAMP JAB.

Large Government Systems Integrator Defensive Cloud Solutions

1. **Amazon AWS**
   While we see Amazon's desired cloud dominance as the "market-maker," we enthusiastically welcome the disruption they are causing to the overall economics of computing. Our ARC Oven offerings do not merely allow us to provide an alternative to AWS, our ARC Oven, more significantly, allows our teaming partners to successfully compete with AWS with a variety of superior resources, networking, customization, security and customer service.

   It has clearly become Amazon versus Autonomic Resources as the two dominant options in the FedCloud Ecosystem. Autonomic Resources, however, has more flexibility. Examples include tailoring and integrating management tools into on premise environments [try that with Amazon, good luck] to customizing per agency as needed. Amazon has to serve the masses as well as provide a uniform service to all of the public sector. Autonomic Resources has the flexibility, and all companies [be it

public sector or not] want their own spin on things. The FedRAMP authorization process demands customization, and this is where we exceed all of Amazon's capabilities.

2. **Microsoft Azure**
   Microsoft's Global Foundation Services [GFS] cloud infrastructure is the data center and network engine that powers Microsoft's enterprise cloud services. Azure is accredited by FedRAMP for both IaaS and PaaS, but it limits customer choices as it is fundamentally focused on Microsoft technologies and development tools.

3. **Lockheed Martin**
   Lockheed Martin SolaS Cloud is a government community cloud computing platform. SolaS Cloud was built to meet FISMA Moderate and FedRAMP certification requirements. SolaS offers Infrastructure as a Service [IaaS] Virtual Machine [VM] cloud services utilizing an on-demand pricing model.

4. **General Dynamics Information Technology** [GDIT]
   The GDIT OMNI Cloud is currently in FedRAMP processing for IaaS accreditation.

5. **CGI Federal**
   CGI Federal was not far behind Autonomic Resources in it's provisional ATO for IaaS community cloud offering. While their IaaS offerings are similar to those of Autonomic Resources, their large size makes them far less responsive to the evolving Federal Cloud Ecosystem.

6. **HP**
   HP received a provisional ATO at the moderate level from JAB for it's Helion IaaS.

7. **IBM SmartCloud**
   The IBM Smartcloud is built on a collection of IBM technologies to perform cloud-like computing capabilities. It has yet to be FedRAMP accredited and prompted IBM to purchase Softlayer as an alternative cloud platform.

Traditional telecommunications and data center hosting companies are trying to find the footing as new cloud models become the dominant form of computing architecture. Although the NIST definition is very specific as to what is considered cloud computing in the Federal marketplace, many of the competitive offerings being promoting are merely managed colocation and hosting services dressed up as cloud.

This "cloud-washing" is pervasive among traditional IT suppliers who have not effectively addressed the transition to cloud based architectures. Although there is room for this approach in the market as some customers will elect to start with a managed off-premise approach, no other supplier has positioned itself to capture this component of the market as effectively as Autonomic Resources.

Managed Hosting and CoLocation Masquerading as Cloud

1. **Verizon**
   Verizon Terremark provides IaaS in the form of traditional colocation for the Federal government. This system utilizes virtualization technology from VMWare, as well as compute and network infrastructure from traditional technology suppliers Cisco and NetApp.

   Verizon Terremark has applied for but yet to receive FedRAMP Authorization for their community cloud. They have a current strong market position in DoD through traditional off-premise computing contracts. While Verizon Terremark reportedly has built out hybrid and private cloud solutions, these products are not yet accredited by FedRAMP.

2. **CenturyLink**
   CenturyLink Savvis provides IaaS in the form of traditional colocation for the Federal government. They have applied for but yet to receive FedRAMP Authorization [level moderate] for their community cloud.

H. Architecture and Relationship Advantages

Starting in 2009, with global industries and the Federal government shifting to a cloud-centric computing model, Autonomic Resources made a strategic change in investment and organizational focus. In light of this dramatic market shift, we abandoned the dated system integrator strategy by creating a "product development oven" capable of incubating and launching certified-secure cloud offerings for the government's inevitable migration to the cloud.

Since then, we have maintained a determined focus on the creation of intellectual property, unique contract vehicle acquisition, programmatic supply chain relationships, and brand creation. This unprecedented strategy has resulted in a uniquely unassailable position in the emerging FedCloud Ecosystem.

With our ARC-P platform, we are widely recognized in the Federal Government service provider sector as a unique cloud innovator. We have built a singularly distinctive reputation for utilizing government initiatives, mandates, and strategies to develop an architecture uniquely tailored to satisfy the government's cloud mission objectives. We are well known among all government agencies and by notable hardware, software, and systems integration companies for our constant innovation, astute understanding of regulatory and procurement guidelines, and our successful determination to achieve accreditations.

We have established our unique position in the FedCloud Ecosystem by creating an exceptional architecture built in conjunction with industry leading partners.

1. **Exceptional Architecture**

Our ARC-P cloud architecture is described as a multi-cloud delivery platform providing access to a multi-cloud stack with the ARC-P security boundary. Our technologies include: Red Hat Enterprise Virtualization [RHEV], Red Hat OpenStack [RHEL OSP], Mirantis OpenStack with Trusted Execution Pools [Intel TXT], and Citrix XenDesktop for VDI with Trusted Execution Pools [Intel TXT].

No other cloud service provider has taken this broad based multi-cloud management approach to defining, certifying, and launching FedRAMP certified cloud offerings in support of the Federal government's "cloud first" computing initiatives.

In addition, our approach provides for full API integration to other certified cloud offerings that are sure to be components of large enterprise multi-cloud computing environments. This approach allows for the development of hybrid cloud environments with multiple cloud platforms being utilized based on function, price, accessibility performance, and customer preference.

ARC-P aims to be the control panel through which cloud compute resources are provisioned and managed. Our current API integration initiatives include orchestration to multiple Openshift variants, Amazon AWS Cloud, Microsoft Azure Cloud, and on-premise VMware environments. This management platform will provide a single management domain to systems integrators and customer agencies to manage assets within the ARC-P security boundary.

The ARC-P IaaS and related platforms have been designed and implemented upon a technology stack that is largely open source in nature. The result of that design has allowed ARC-P to be priced to customers at approximately one-third of the cost of existing Federal Cloud providers, as well as maintain competitive pricing with Amazon Web Services.

By incorporating open standards [aka open source] software, ARC-P easily facilitates:

- ➔ Multi-cloud management API's integrations.
- ➔ Integration of cloud monitoring and security with existing IT service management systems and multiple hypervisor support.
- ➔ Ability to virtualize in the cloud both AIX and System Z operating systems.
- ➔ Extensive use of OpenStack's multi variants via Mirantis and Red Hat OpenStack.

2. **Unique Supplier and Teaming Partner Relationships**

Autonomic Resources' position in the Federal Cloud ecosystem has been further enhanced by the deep and unique relationships we have established with software and hardware manufacturers that look to us to assist in giving them a channel to access the Federal cloud computing spend. We serve as their enabler to distribution in a cloud-based marketplace. ARC-P, as a distribution conduit, allows these manufacturers to deliver products to be consumed by end-user agency customers in the new cloud computing paradigm.

These key relationships include Red Hat, IBM, Microsoft, Dell, Citrix, NetAPP, Akamai, Super Micro, Mirantis, Hitachi Data Systems, MongoDB, and Jaspersoft, amongst others. These companies look to us to assist them

in delivering their products in a utility based compute “as a service” model that is favored by government agencies seeking to move to an opex [operating expense] driven subscription model for budgetary reasons.

Additionally, Autonomic Resources has been instrumental in assisting these companies in redesigning licensing programs and sales compensation models as the old programs are being disrupted in the new cloud-based model. In most cases, we have arranged for these manufacturers to continue to give quota relief to their Federal sales teams for spend that occurs between agency and Autonomic Resources. This strategy has allowed us to have, by default, access to a potentially large and experienced Federal sales force that extends well beyond the Autonomic Resources internal sales and contract capture team.

We are now in the enviable position of both provoking and benefiting from the massive disruption in the computing supply chain as cloud computing fundamentally changes all traditional relationships, behaviors, and approaches to the delivery of solutions to government customers.

- ➔ Since ARC-P achieved FedRAMP certification in December 2012, Autonomic Resources has been invited to join multiple IDIQ, BPA, and GWAC contracts via existing Prime vendors. Prime contract holders wish to assure they have an approved and cost effective CSP on the team as task orders are released under those vehicles seeking FedRAMP accredited Cloud services.

- ➔ Our position as an independent CSP has also positioned us to be an “exclusive” CSP partner in key agency cloud contracts by large SI Primes who have large revenue streams at risk in those agencies.

I. Company Overview and Financial Projections

Autonomic Resources is a limited liability company registered in North Carolina. The company is independently owned, closely held, and operates as a partnership not influenced by any outside corporate investors. Our founding partner, John Keese, serves as the company’s cloud technology visionary and sets product development direction. Our managing partner, Tom Thomson, is accountable for investments, operations, and financial performance.

John Keese, Tom Thomson, and our sole investment partner, Walker Global Solutions, collectively own 100% of our outstanding shares. There are no other current options, warrants, unit appreciation rights, convertible securities, or other equity interests in Autonomic Resources. Autonomic Resources has no active or pending litigation.

Prior to founding Autonomic Resources, John Keese’s experience included executive leadership in business development for a large commercial technology services firm and as a Corporate Information Director for a large regional security firm in the New York. John is the former chairman of the Open Software Institute, and he is currently a member of the Cloud Computing Caucus and a Commissioner on TechAmerica’s Commission on the Convergence of Technology.

John is continuously accessed by industry analysts as an expert in the areas of Federal Government Cloud computing strategy and secure Cloud computing. He is well known in the software and hardware supplier markets as an innovator, in particular in the areas of open standards, open source software, and cloud computing.

Autonomic Resources was founded in 2001 in Raleigh, NC [originally under the name Advantage Professionals of Raleigh, LLC]. Since 2009, we have transformed our company from a traditional systems integration and IT services firm into the innovative and leading edge cloud service provider it is today. Through the ARC Oven, Autonomic Resources has developed the intellectual capital and process capability to identify, architect, develop, accredit, and launch comprehensive set of cloud based infrastructure, platform, and software offerings broadly referred to as part of the ARC-P platform. The ARC-P platform includes a full suite of offerings comprised of Infrastructure as a Service [IaaS], Platform as a Service [PaaS], Email as a Service [EaaS], and multi-cloud management, among others.

The ARC-P approach was intentionally developed to address the Federal Government’s Cloud computing directives, and this was rewarded when the we achieved first mover advantage through the first FedRAMP with

the first Provisional ATO for its ARC-P Infrastructure as a Service [IaaS] offering. Subsequently, we have continued to execute on our successful strategy to develop, certify, and launch FedRAMP certified products. These offerings are key to IDIQ and task order capture as government agencies begin to demand that cloud offerings be FedRAMP accredited.

Autonomic Resources is headquartered at our 2,500 square foot facility in the Raleigh-Durham Research Triangle area. Autonomic Resources pays market rates for a continuous term lease from Cascade Pointe LLC, a wholly owned subsidiary of Autonomic Resources. The lease terms include a mandatory 12-month cancellation notice. **Autonomic Resources,** 200 Cascade Pointe Lane, Suite 103, Cary, North Carolina 27513

Additionally, Autonomic Resources leases data center facilities in both Ashburn, VA and Atlanta, Ga. These facilities provide over 450,000 square feet of secure space allowing for significant expansion of the existing ARC-P IaaS footprint. We have built out our leased space to the exacting standards of FedRAMP for our provisional ATO.

The partners of Autonomic Resources also hold interests in other companies that provide shared services to Autonomic Resources. Consilium Global Management of Williamsville, NY provides back office support and provides all of Autonomic Resources' accounting and billing functions. Additionally, when the need arises, Autonomic Resources leverages the capabilities of Consilium1, a cloud service provider, systems integrator, outsourcing, staffing, and cloud security consulting firm specializing in the commercial and healthcare IT industries.

Affiliations and Memberships

Cloud Computing Caucus Advisory Group
The Cloud Computing Caucus Advisory Group is a non-profit, non-partisan coalition of technology companies and industry groups focused on educating lawmakers and the public about cloud computing as well as other information technology issues . Autonomic Resources is a Silver Supporter of the Cloud Computing Caucus and is active in the quarterly Hill-versation Caucus meetings held in Washington DC.

Red Hat Certified Cloud Provider
As a Red Hat Certified Cloud Provider, Autonomic Resources runs Red Hat technologies on certified and supported virtualization solutions, ranging from Red Hat Enterprise Virtualization to VMware to Microsoft solutions. The first of its kind in the industry, Red Hat's Certified Public Cloud Provider Program provides partners with access to a comprehensive family of Red Hat software and solutions to build out a cloud infrastructure. The program includes services that are designed to build the foundation for your Red Hat offerings and to quickly start delivering Red Hat solutions on your cloud.

The Open Source Software Institute
Autonomic Resources is a Platinum Member of the Open Source Software Institute. The Open Source Software Institute is a U.S.-based 501[c][6], non-profit organization whose mission is to promote the development and implementation of open-source software solutions within US Federal, state and municipal government agencies. OSSI was established in 2000, and has focused on strategic initiatives to promote the adoption of open source within US Department of Defense and Department of Homeland Security.

The Linux Foundation
Autonomic Resources is proud to be a Silver Member of the Linux Foundation, a host of the Open Virtualization Alliance special project. The Linux Foundation helps companies and individuals navigate the ever-changing landscape of Linux and other open source initiatives.

The Open Virtualization Alliance
The OVA provides education, best practices, and technical advice to help businesses understand and evaluate their virtualization options. The consortium complements the existing open source communities managing the development of the KVM hypervisor and associated management capabilities, which are rapidly driving technology innovations for customers virtualizing both Linux and Windows® applications. The OVA is not a formal standards body and does not influence upstream development, but encourages interoperability and the development of common interfaces and application programming interfaces [APIs] to ease the adoption of KVM for users.

North Carolina Technology Association
The North Carolina Technology Association's mission is Making North Carolina Number One in Technology and Technology Number One in North Carolina. The organization does this through three main focus areas: executive engagement, public affairs and knowledge workforce.

Key Products and Professional Services

Autonomic Resources ARC Oven utilizes industry standard open source technologies such as KVM and OpenStack in the development of our cloud platforms. The ARC-P platform is flexible, highly secure, and extensible, allowing for eased customer adoption and consistent FedRAMP acceptance. Our cloud offerings are cost effective, highly adaptive, and secure.

ARC-P IaaS-Community

The ARC-P Community Cloud is a KVM-based cloud service that provides for physical or virtual machines, as well as other resources while ensuring interoperability and support for multiple hypervisor images. ARC-P Community Cloud also offers additional services, including virtual machine disk image libraries, block and file-based storage, firewalls, load balancers, IP addresses, VLANs, continuous monitoring services, and software bundles. ARC-P IaaS received a FedRAMP Provisional ATO in December 2012 [ATO number]. ARC-P received a DISA ATO at Impact Levels 1 & 2 in April 2013.

ARC-P IaaS-Private

The ARC-P Private Cloud is similar to the ARC-P Community Cloud in the scope of its service offerings. However, the Private Cloud supplies elastic compute resources from ARC-P pools installed in our CONUS-only data centers. ARC-P IaaS received a FedRAMP Features include automated provisioning, charge-back and quota controls, workload portability between on premise, community and public clouds. This allows agencies to manage their on premise virtualized assets as well as securely connect to FedRAMP accredited cloud service providers, and public clouds, like AWS, from a single management domain. Additionally it will allow for disposable resources, heterogeneous cloud management, and an operational expense model.

ARC-WRX PaaS

Our ARC-WRX Platform as a Service offering is based on OpenShift by RedHat. Directed at the development community, OpenShift allows for rapid spin up of IT development environments within the ARC-P environment connected to the customers IT environments whether in the ARC-P boundary or outside that boundary. We are the ONLY provider of OpenShift as a Service in the CONUS, outside of the openshift.com environment. This environment is in FedRAMP processing for authorization.

Email as a Service

Email as a Service [EaaS] is represented by the Microsoft Office 365 platform, Government Community Cloud Edition.

Business Intelligence and Data Analytics

Autonomic Resources will be enabling a business intelligence and data analytics as a service platform in collaboration with open source partners Jaspersoft and MongoDB. This platform will be brought through the FedRAMP accreditation process after build and evaluation completion in early 2015.

Security Processing and Continuous Monitoring

The Autonomic Resources team assists ARC-P Cloud ecosystem partners in Security Package Development Security Risk Assessment/Testing, Security Assessment Planning [SAP development], and Managed Security Services Scanning and Reporting [continuous monitoring services]. FedCloud Express also provides consulting services to PaaS and SaaS partners in preparing security packages for review and certification by a Third Party Assessment Organizations [3PAO].

FedCloud Express Professional and Managed Services

While the ARC Oven's strategy remains focused on the incubate, build, certify, and launch cloud platform process, our FedCloud Express business unit offers a comprehensive suite of FedRAMP certification services.

Traditionally, infrastructure outsourcing managed services assume agencies grant systems integration and management contracts using a "basis of estimate" tied to the physical server to systems administrator traditional computing models. These models are being disrupted by the elastic compute and "XaaS" operating expense models that support Cloud computing. Our position at the center of the FedCloud Ecosystem enables contract acquisition around new models for services including systems monitoring, help desk support, application support, backup and recovery management, patching and maintenance of operating systems and application support and maintenance.

Clients for managed and professional services will naturally come from the FedCloud Express customer base. Application modernization and migration to the Cloud objectives are critical for agencies to sustain and grow in an increasingly demanding climate. FedCloud Express offers a full range of cloud professional services for cloud readiness assessment, strategy development, and roadmap for replatforming and migration including:

- ➔ Dedicated services for migrations, deployment, and testing [replatforming].
- ➔ Software development and cloud refactoring services.
- ➔ Cloud assurance services for quality deployments.
- ➔ On-going performance tuning, software enhancement, and systems maintenance services.
- ➔ Decommissioning of legacy applications and data centers.
- ➔ Cloud Enabled Managed Services.

Autonomic Resources is successful in securing strategic contract vehicles as a prime, as well as providing complementary services as a team member to prime contractors where there is a strategic value to contracts. We are continually evaluating new teaming requests as many current prime contract holders are looking for ways to include cloud computing offerings under current contracts. These arrangements will continue to add to an already formidable list.

Total Addressable Market

Cloud computing is growing significantly as a percentage of the Federal Government's shrinking IT budget in the coming years as the culture shifts from an asset-based to an "as-a-service" mindset. It is projected that cloud-related expenditures by Federal agencies will grow to an estimated **$7.30 billion** by 2018. In fact, 94% of respondents to TechAmerica's 2013 Federal CIO Survey said their agencies have or will adopt public or private cloud services. The key drivers continue to be the cost savings, flexibility, and the operational efficiencies that cloud computing provides. It is our intention to maximize the potential of the unresolved FedCloud migration.

Key Historical Milestones

1. Autonomic Resources is awarded GSA IaaS BPA contract award in March of 2011
2. Autonomic Resources is first to FISMA moderate ATO , December 2011
3. ARC-P is first FedRAMP accredited IaaS Platform, December, 2012
4. Autonomic Resources awarded Prime Contractor award on 10 year, $10 billion Department of Interior Cloud Foundation IDIQ GWAC contract, May 2013
5. ARC-P Private is first FedRAMP accredited for IaaS and DaaS, June 2013
6. Autonomic Resources announces Powered by ARC-P Reseller Program, July 2013
7. Autonomic Resources announces ARC-PE Exclusivity program for Technology and Systems Integration Teaming Partners, August 2013
8. Autonomic Resources launches FedRAMP Security and Application and Application Re-platforming Consulting Services, September 2013
9. Autonomic Resources is first to receive DoD-wide Iaas Provisional ATO from DISA at Impact levels 1 and 2, November 2013
10. Autonomic Resources and Hitachi Data Systems Federal announce strategic cloud go-to-market strategy, December, 2013
11. Autonomic Resources is first to FedRAMP annual reauthorization, January 2014
12. Autonomic Resources becomes Founding Member of Federal Cloud Computing Caucus Advisory Group, January 2014
13. Autonomic Resources named Red Hat Public Sector Partner of the Year, January 2014
14. Autonomic Resources IaaS FedRAMP Authorization is first to be leveraged for JAB Authorized SaaS ATO [CTC], January 2014
15. Autonomic Resources joins Linux Foundation and commits to Open Virtualization Alliance, February 2014
16. Autonomic Resources and Akamai Technologies are First layer FedRAMP Authorizations for Unprecedented Control in Public Sector Cloud, March 2014
17. Autonomic Resources launches FedRAMP Express program providing agencies and SaaS providers unprecedented access to leverage ARC-P IaaS ATO, June 2014.
18. Autonomic Resources launches Continuous Monitoring Services for sustaining government cloud compliance, July 2014.
19. Autonomic Resources becomes founding member of TechAmerica's Commision on the Convergence of Technology, August 2014.
20. Autonomic Resources receives FedRAMP approval for physical control decoupling of the ARC-P IaaS ATO enabling creation of ARC Secure Data Centers, imminent October 2014.
21. ARCWRX PaaS platform receives FedRAMP JAB ATO, anticipated December 2014

Pertinent Articles

Posted by: MarketsandMarkets.com
Publishing Date: August 2013
Report Code: TC 2035

The Enormous Potential of the Government Cloud

Government Cloud has a long-term potential as it brings greater efficiency to government organizations IT and service delivery segment. The main benefit of public cloud is that government and public bodies are offered high elasticity and reduced costs for running the applications. Federal, State and Local, and Defense and Military are widely embracing cloud service as it helps in collecting and managing huge amount of data. The most important thing that these government agencies require is a cloud that has effective and able developers to easily integrate it with other parts of the infrastructure.

The consolidated information in the government cloud saves millions of dollars each year with the adoption of cloud applications such as server and storage, collaboration, business operations, disaster recovery/data backup, health and safety, security and compliance, mobility, analytics, cloud gaming and content management.

The Government Cloud market is segmented on the basis of delivery modes comprising of Infrastructure as a Service [IaaS], Platform as a Service [PaaS], and Software as a Service [SaaS]. Government and other public bodies are likely to purchase more and more of infrastructure and software services from the cloud stores. IaaS is the most popular offering in government cloud, closely followed by SaaS and other development services. The leaders in the market are investing in acquisitions and new technologies to enrich their existing product portfolio and address the increasing demand across a wide range of public and government organizations.

The Federal Cloud Market is expected to accelerate through the forecast period, ranging from $1.26 billion in 2013 to $7.30 billion in 2018, at the CAGR of 42.2% during the forecast period.

Amongst the delivery modes, the market size for IaaS delivery type in the Federal Cloud Market is expected to grow from $579.5 million in 2013 to $3.26 billion in 2018, at a CAGR of 41.3% during the forecast period. The market size of SaaS delivery type is expected to grow from $387.2 million in 2013 to $2.62 billion in 2018, at a CAGR of 46.6% during the forecast period. The IaaS delivery type is expected to grow from $412.8 million in 2013 to $2.60 billion in 2018, at a CAGR of 44.6% during the forecast period. While the SaaS delivery type is expected to grow from 275.8 million in 2013 to $2.09 billion in 2018, at a CAGR of 50% during the forecast period.

SearchCloudSecurity.com

Is FedRAMP the cloud security standard we've been waiting for?

The Federal Risk and Authorization Program was launched in June 2012 to support the adoption of standardized cloud services among federal agencies in response to President Obama's "cloud first" policy -- a move intended to reduce the government's IT spending by cutting the number of data centers in use and sharing computing resources.

To continue working with the federal government, cloud service providers [CSPs] had to apply for an authorization to operate [ATO] via either the FedRAMP Joint Authorization Board [JAB] or directly through a government agency by June 5, 2014. It's a feat that 12 CSPs have completed to date -- Autonomic Resources, Akamai Technologies, Amazon Web Services, HP, IBM, Lockheed Martin, Microsoft and Oracle among them -- **with dozens more stuck in a lengthy queue**.

While FedRAMP was created to save federal agencies both time and money, the accreditation program has been touted in some corners as a standards-based cloud security approach that could serve as a model for other CSP environments.

In June, FedRAMP director Maria Roat said contacts from private industry and governments around the world are looking to build standards-based security programs on the back of FedRAMP. Such a development may prove vital to the cloud industry, as security has remained the number one concern for most organizations offloading services to cloud environments.

FedRAMP accreditation promises to ease security concerns by ensuring cloud environments maintain a proper security posture. Joe Vehemente, the service line manager of Akamai Technologies' federal division, said FedRAMP was one of the "broadest and deepest security commitments" his company has ever made. The content delivery and cloud infrastructure services provider was granted a provisional ATO in 2013, a feat that will have to be consistently repeated through monthly, quarterly, and yearly reviews due to the continuous monitoring aspect of the program.

"Going through the process, we actually had to document all of our responses to all the security controls within the FedRAMP baseline," said Vehemente, noting the demands of the rigorous FedRAMP documentation process. "It definitely strengthened our security posture to where we had to make sure we were dotting our i's and crossing our t's."

FedRAMP's security controls are based on guidance from the stringent National Institute of Standards and Technology Special Publication 800-53 Revision 3, which has been used throughout the federal government for years. FedRAMP 2.0 -- the update to the cloud program that was finalized only days after the initial June deadline had passed -- toughens the requirements laid out by making corresponding changes to align with revision 4 of NIST SP 800-53, released in April 2013.

The FedRAMP program ratchets up the standard of security expected of cloud providers to the point that even government entities, like the Department of Defense that maintain the strictest security requirements, can now utilize cloud services. Department of Defense CIO Teri Takai, who serves on the FedRAMP JAB, has signaled in recent interviews that FedRAMP is helping shape how cloud providers implement security controls to the point that the government has had to offer a branding guide for FedRAMP-certified providers.

The FedRAMP accreditation raises the bar for cloud security standards, but only certain organizations -- read: U.S. government agencies -- are actually able to take advantage of the security benefits of the government's program right now, said David Escalante, director of computer security and policy at Boston College.

Escalante said that he would be interested in moving his hosted services to cloud environments that have undergone the FedRAMP authorization process, but current FedRAMP-certified providers haven't subjected all of their services to the accreditation process. IBM offers numerous cloud services, for example, but only its infrastructure as a service SmartCloud for Government is currently FedRAMP-certified.

"I do think a provider getting a FedRAMP ATO speaks to its commitment to security and compliance," said Stu Fleagle, vice president of government solutions for managed hosting and cloud provider Carpathia, which is currently undergoing the U.S. government's authorization process in collaboration with VMware for an enterprise hybrid vCloud service.

Richard Santalesa, founding attorney with the Sm@rtEdgeLaw Group, in Fairfield, Connecticut, said there are still ways that private organizations can take advantage of FedRAMP standards. He advises clients to push for the inclusion of the same security controls in contract negotiations with cloud providers, using the FedRAMP Standard Contract Language as guidance.

"In some cases, we were able to get basically the same functionality, not necessarily the FedRAMP stamp, but essentially the same parameters," he said. "And in one successful case, a client was basically able to utilize the same FedRAMP contracting language because a federal agency had just utilized [the cloud service provider]."

As to whether FedRAMP accreditation can become a de facto security standard across the cloud industry, Santalesa cautioned that it is still early days for the federal program. Several of the law firm's clients within the critical infrastructure sector have already taken an interest in FedRAMP-certified cloud services due to the overlapping guidelines in the NIST SP 800-53 and the NIST cybersecurity framework, which was released in February.

Autonomic gets DoD FedRAMP OK

By Frank Konkel November 14, 2013

Autonomic Resources, the first cloud provider to achieve compliance under the Federal Risk and Authorization Management Program [FedRAMP] back in December 2012, has now become the first to achieve additional security control required by the Department of Defense.

Autonomic announced it was issued a provisional authorization by the DoD on Nov. 12 for its Autonomic Resources Cloud Platform [ARC-P] infrastructure as a service offering, making it the only cloud provider offered for DoD-wide acceptance under the Defense Information Systems Agency [DISA] Enterprise Cloud Service Broker catalog.

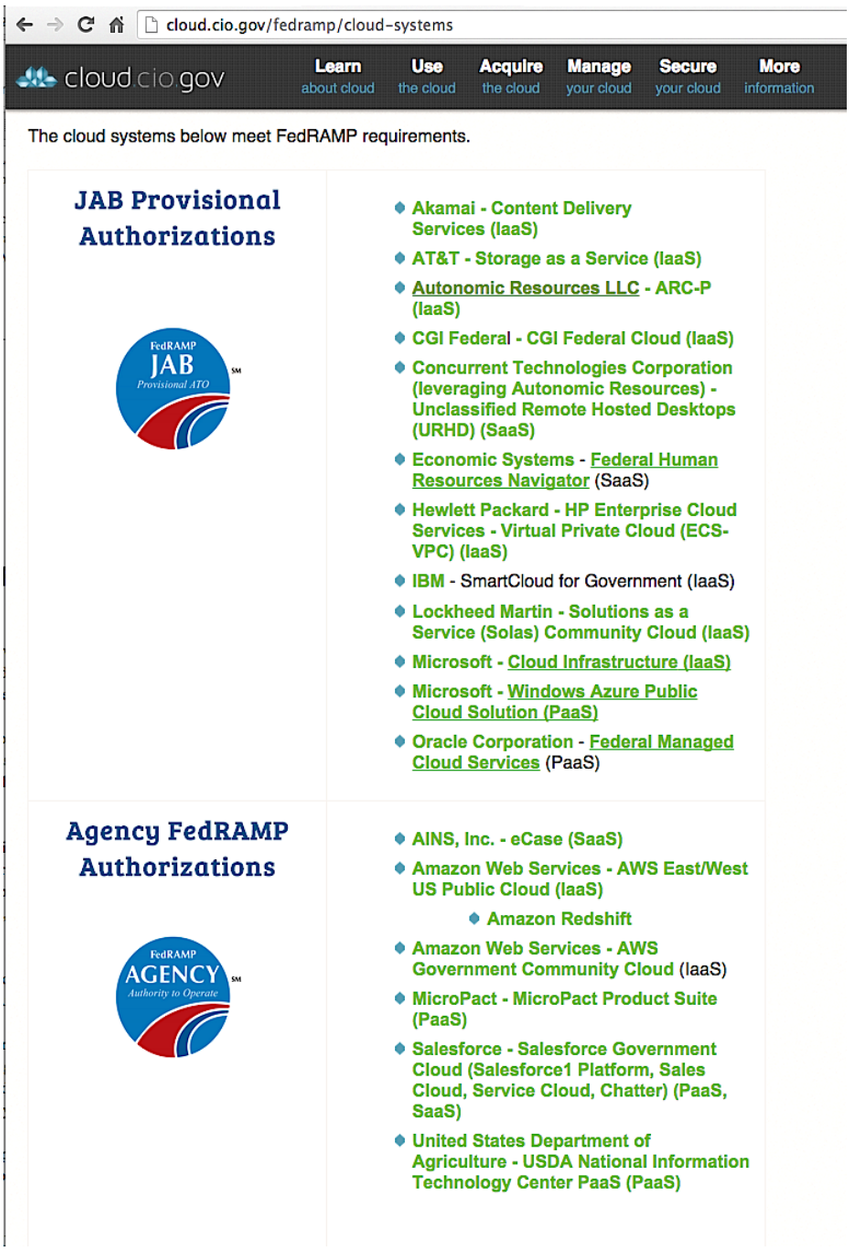
After ARC-P achieved FedRAMP compliance, it was further assessed using the DoD cloud security model, taking into account an additional 23 controls and enhancements from third revision of the National Institute of Standards and Technology Special Publication 800-53. According to Autonomic, ARC-P is now authorized at DoD Impact Levels 1 and 2, meaning it is approved for unclassified public information and unclassified private information.

"ARC-P is yet again first in security authorizations that are meaningful to our government cloud customer," said John Keese, President and CEO of Autonomic Resources.

"The ability to leverage our FedRAMP Provisional ATO, granted by the Joint Authorization Board, assisted DoD in rapid approval, something that would have been much more difficult with a single agency FedRAMP compliant ATO," Keese added in a statement. "Additionally, ARC-P is ready for authorization at Impact Levels 3 and 4 once finalized by DISA, and Level 5 by early 2014."

A provisional authorization is an initial approval for a cloud service provider's platform by the DISA Designated Accrediting Authority. That body can then use the provisional authorization to grant specific customers an authority to operate.

Thus far, 10 providers have achieved FedRAMP compliance, including Autonomic. The FedRAMP Joint Authorization Board has granted seven other cloud providers provisional authority to operate: Akamai, AT&T, CGI Federal, Hewlett-Packard, IBM, Lockheed Martin and Microsoft.



SearchCloudSecurity.com

As FedRAMP deadline nears, slow approvals leave CSPs in the queue

29 May 2014

Cloud service providers that deliver services to U.S. government agencies are required to gain FedRAMP accreditation by the upcoming June 5 deadline, yet dozens of CSPs are stuck in a slow-moving security-driven approval process that could result in fewer providers competing for the government's cloud computing contracts.

Originally announced in 2011, the Federal Risk and Authorization Management Program [FedRAMP] was created to standardize security requirements for cloud service providers [CSPs] vying for contracts with federal agencies. The intent with FedRAMP is to reduce the time and money agencies spend on redundant cloud provider security assessments in favor of a single accreditation.

The reality is, the government is not going to function without this technology.

Interested CSPs can apply for an authorization to operate [ATO] via either the FedRAMP Joint Authorization Board [JAB], under the General Services Administration umbrella, or directly through the government agency utilizing the services. To date, more than a dozen cloud providers have successfully attained FedRAMP approval, including Autonomic Resources, Amazon Web Services, Microsoft and Hewlett-Packard Co.

The U.S. government's FedRAMP website lists dozens of additional CSP requests still working toward authorization, including Google, Salesforce.com, Verizon and other major cloud providers. In fact, the requests of eight providers -- AT&T and Dell among them -- are listed as "ready for kickoff," meaning they have yet to begin their review processes.

Waylon Krush, CEO of Arlington, Virginia-based Lunarline Inc., a certified FedRAMP third-party assessment organization [3PAO], said he was surprised that more CSPs haven't successfully navigated the process, especially considering the government has been actively warning that the FedRAMP deadline was approaching. Krush said CSPs may have been slow in their uptake of FedRAMP because government-based cloud customers had not been forceful enough in requests that providers adhere to the guidance, though he saw that attitude shift toward the beginning of 2014.

"These CSPs aren't necessarily going to go out and invest in the necessary infrastructure and the ability it takes it to secure their infrastructure for FedRAMP unless it's required to make a dollar," Krush said. "We're seeing a lot more inquiries now because CSPs are finally hearing customers say, 'No, you do need to go through FedRAMP, and if you don't, there's a chance you may not get this contract.'"

FedRAMP deadline consequences

Though dozens of CSP requests are currently in the FedRAMP queue, Robert Barnes, a director and public sector practice leader with Coalfire Systems Inc., a certified FedRAMP 3PAO based in Louisville, Colorado, tempered expectations for a tidal wave of authorization approvals. That's because the review process can take several months to complete on average, with the assumption that no significant issues are encountered.

Why so long? Barnes said the FedRAMP review team -- composed of six information system security officers [ISSO] and a limited number of JAB technical representatives -- only has so much bandwidth available to handle CSP requests. That bandwidth is further restricted by the fact that CSPs who currently have an ATO must also be reassessed on a yearly basis, and according to current FedRAMP guidance, those providers will take precedence over other, as-yet-uncertified CSPs in the queue.

Furthermore, a CSP's authorization process may be delayed if it is unprepared to meet the demanding FedRAMP requirements, Barnes said. For instance, if an assessment uncovers "high-risk" vulnerabilities in a provider's environment, it could take weeks or months to remediate the flaws and then schedule a 3PAO reassessment.

All told, it could take years just to clear the current FedRAMP JAB queue, Barnes said, without counting the CSPs that have yet to even begin the process.

"It truly is a marathon. You've got cloud service providers who trained up. They have a nice program and risk-management framework in place; they've got the controls; they've got the documentation; they did all the preparation and training. And then they went through the process that took them six to nine months to gain that ATO at the end of the race," Barnes said. "Those that are actually in the queue today are actually in really good shape, as opposed those that are just starting to think about what is FedRAMP."

From the CSP perspective, Barnes said providers that haven't gained a FedRAMP ATO are simply not going to be competitive for government contracts going forward. "We've heard from cloud service providers that contracts are now very much reflecting FedRAMP as a standard or requirement, that business can't be won or achieved without receiving an ATO, and that's starting to become a reality for a lot of these companies that didn't necessarily start two years ago when the FedRAMP program was initiated," Barnes said. "Those who have existing contracts though, or are looking to expand on the business they already have, they could lose business -- either to [a] competitor that has a FedRAMP authority to operate, or to those that are ahead of them in the queue."

The possibility of being locked out of bidding for government contracts combined with the upcoming FedRAMP guidance changes may result in a desire from some CSPs to rush through the process, but Krush warned such organizations that FedRAMP requires an "eye-opening" cultural change from a security perspective, and that can't be hastened.

"CSPs need to know this doesn't happen in a day. This is not one of those fire and forget processes, meaning you can just put a jumble of documentation together, throw it at the FedRAMP JAB or organization sponsor and expect to be authorized," Krush said. "This requires ongoing and continuous monitoring. This requires you to

have a very strong configuration management control process, content scanning and patch updates at a level that is surprising even to organizations that are used to dealing with the depth and rigor of government controls."