



# COMPLIANT SOLUTIONS

Software-as-a-Service (SaaS)

Security and Compliance-Driven Infrastructure Considerations for  
Software/SaaS Firms Targeting Public Sector Organizations





## Contents

<b>Executive Summary</b> .....	1
<b>Introduction</b> .....	3
<b>A Working Definition of Government-Compliant SaaS</b> .....	5
<b>Key Technical Differences and Requirements in Delivering SaaS to Government Customers</b> .....	7
<b>Key Business Differences and Requirements in Delivering SaaS to Government Customers</b> .....	11
<b>Benefits of a Federally-Compliant Infrastructure Partner</b> .....	13
<b>Recommendations for SaaS Providers that Target Public Sector Organizations</b> .....	15
<b>Conclusion</b> .....	16
<b>About Carpathia Hosting</b> .....	17

# Executive Summary

As the Software-as-a-Service (SaaS) delivery model has matured in both acceptance and adoption in the commercial marketplace, attention has turned to Government market, which offers a similarly lucrative opportunity. In fact, according to a recent INPUT U.S. Government Market survey, more than 78% of Federal Agencies stated that SaaS is actively utilized or is under evaluation for various applications.

The challenge that exists for Software/SaaS vendors in addressing the Government-compliant SaaS market is twofold. First, most software vendors admit that the IT operations of a hosted environment are not a core strength or competency. Secondly, few, if any software firms understand the additional requirements that must be satisfied in order to achieve a Government-compliant delivery platform.

Government-compliant delivery of software-as-a-service is a niche discipline that coalesces (a) knowledge and best practices from technical and compliance-related areas such as facilities, networking, systems, data/storage, physical/logical/procedural security, monitoring, reporting, identity management, media handling, and many others, with (b) a series of stringent and complex IT security regulations such as FISMA, DIACAP and OMB directives that are mandated and audited by law or are otherwise required operating practice for many Government organizations. **Software/SaaS firms must meet these regulatory requirements in a certifiable manner as part of their qualifications to legally and effectively provide SaaS services to many organizations within the public sector.**

More specifically, Software/SaaS firms must develop, outsource, or otherwise acquire a Government-compliant SaaS delivery platform that addresses a multitude of delivery characteristics including:

- Where the services are delivered (locations and facilities).
- What citizens/personnel have access to the environment (physical or remote).
- What policies and procedures are followed regarding management of the environment.
- How breaches in security or other lapses in procedures are identified, reported and remediated per required Government standards.
- What visibility into the delivery of the environment is provided.
- What infrastructure and application-level security measures exist (including how the Government's data and systems are accounted for and/or separated from other customer infrastructure) for certification and accreditation purposes.
- Other security, process/procedural and compliance-related requirements.

Fortunately, a select group of Government-compliant SaaS infrastructure providers, consultants and other outsourcers is emerging that can address this intersection between a scalable SaaS delivery platform and the Federal government's stringent security and compliance requirements. Today,

these solutions are predominantly supported via specialized infrastructure providers with time-tested and proven experience, past performance, and certified delivery for Government agencies.

Software/SaaS providers seeking to capitalize on the growing Government market opportunity need to become aware and informed regarding the range of complex and potentially margin-threatening compliance regulations that will certainly impact delivery infrastructure. This understanding will be useful to a software vendor developing its own offering, or vetting potential partners who claim experience and expertise in this specialized delivery area.

Successful Government-compliant SaaS platform providers will not only achieve the compelling benefits of SaaS for their Government customers to include lowering cost, expediting delivery and improving overall quality of delivery, but will do so in a manner that differentiates their SaaS offerings in a substantiated and sustainable way for the public sector marketplace relative to commercial-grade SaaS providers that may or may not be in compliance.

## Introduction

First, some context: This white paper is not an introduction to Software-as-a-Service (SaaS). There are a multitude of SaaS primers available that describe what SaaS is, and considerations for those wanting to purchase, use, develop, or otherwise consider SaaS as an offering. The purpose of this white paper is to address how software firms and other solution providers can provide SaaS in a manner that is relevant and compatible with Government standards, compliance regulations and other delivery requirements.

While the IT community increasingly views SaaS as a viable and inevitable alternative delivery model for certain business applications, the path leading to public sector adoption and success is proving to be a bit more elusive. This is because public sector organizations – particularly those striving for security and compliance assurance – are still grappling with how to leverage SaaS while still achieving the required security, policies, visibility and accountability to the organizations, stakeholders and U.S. citizens that they serve.

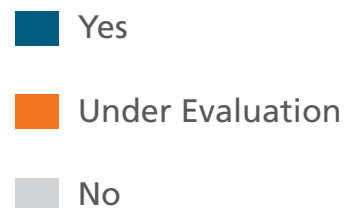
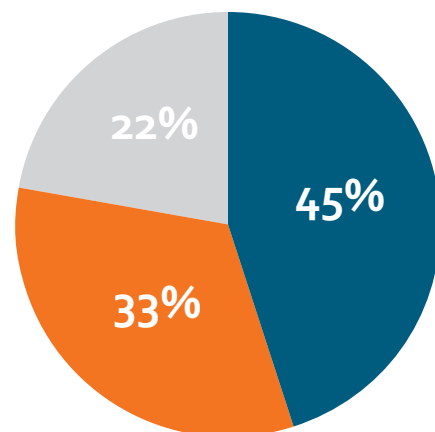
This paper will:

- Provide a working definition of Government-compliant SaaS.
- Highlight key technical and business model differences and requirements in delivering SaaS to Government customers.
- Describe benefits that can be realized through partnership with a Federally-compliant managed infrastructure/hosting provider.
- Offer recommendations for SaaS Providers who target public sector organizations.

Where there are differing opinions regarding the speed of SaaS adoption for small and medium versus large organizations, as well which application/business functions are better suited for SaaS than others, the advantages of SaaS are simply too compelling for most organizations to ignore -- including those within U.S. Government organizations. Specifically, key benefits that have been realized by SaaS customers include:

- Faster deployment times
- Improved quality of delivery
- Reduced cost
- Simplification of client service software installation and maintenance responsibility
- Reduction of workload of internal IT staff or other costly third party outsourcers

### Are you considering SaaS in your company?



Additionally, SaaS delivery presents opportunities for software companies themselves to enhance their value to customers, including more direct control over the implementation and successful delivery of their applications (instead of leaving the desired outcome in the hands of the client or third party integrators).

The leading analyst firms agree. According to analyst firm IDC, SaaS revenues are projected to increase from \$3.7 billion in 2006 to \$14.8 billion by 2011. On the basis of this exploding opportunity, scores of SaaS vendors have emerged to offer Web-based alternatives to the traditional on-premise delivery model.

Most of the customers currently leveraging the SaaS delivery model are private sector companies. That said, public sector organizations across the Federal, State and Local levels are increasingly exploring SaaS for their own missions, programs and other requirements.

In fact, according to a recent INPUT U.S. Government Market survey, over 78% of Federal Agencies stated that SaaS is actively utilized or is under evaluation for various Program applications. (See figure at right.)

The Government market segment is likely to be a very attractive one for software companies with SaaS offerings given the number of users, budgets and mandated requirements of these Government organizations.

In considering SaaS offerings for the public sector, there are important factors that must be satisfied within the delivery infrastructure and application management levels – especially surrounding compliance – that materially differ from conventional commercial deployment assumptions.

As organizations that serve the public sector know, the business of Government is different. These differences need to be embraced, understood and applied to SaaS delivery and support models if software companies hope to effectively sell their managed services to Government entities.

# A Working Definition of Government-Compliant SaaS

U.S. Federal Agencies and other Government organizations are continually seeking more innovative, accountable and cost-effective methods of receiving services, and are increasingly examining SaaS as a viable alternative in the delivery of certain software applications. That said, SaaS is proving to be a foreign concept to public sector organizations accustomed to deploying and managing their software on-premise.

Unlike commercially-oriented SaaS offerings – for which the aspects of where, how, and who is delivering the managed services is subjectively determined by each provider and are rarely externalized, defined or described to their customers – Government agencies procuring services must know (and are required by law to know) at any point in time:

- Where the services are delivered (locations and facilities).
- What personnel have access to the environment (physical or remote).
- What policies and procedures are followed regarding management of the environment.
- What infrastructure and application-level security measures exist (including how the Government's data and systems are accounted for and/or separated from other customer infrastructure) for certification and accreditation purposes.
- How breaches in security or other lapses in procedures are identified, reported and remediated per required Government standards.
- What visibility into the delivery of the environment is provided.
- Other security, process/procedural and compliance-related requirements.

A Government-Compliant SaaS offering (or provider) is one that is able to achieve the compelling value propositions of SaaS and simultaneously satisfy the multitude of security, compliance, and auditable delivery criteria defined by and required for Government organizations.

So do Government-Compliant SaaS platform examples exist that address this intersection between a scalable application SaaS delivery platform and these stringent security and compliance requirements? The short answer is yes, but they are not widely known or advertised. These solutions are predominantly enabled and supported via specialized infrastructure providers with proven experience, past performance, and certified delivery for Government organizations.

## Major Government Mandates/Standards

- **FISMA**, U.S. Public Law 107-347
- **DIACAP**, DoDD 8500.1 and DoDI 8500.2, July 6, 2006
- **NIACAP**, NSTISSC April, 2000
- **NISPOM**, DoD 5220.22-M, February 28, 2006
- **Presidential Decision Directive NSC-63**, Critical Infrastructure Protection, May 22, 1998
- **HSPD 12**, Homeland Security Presidential Directive, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
- **FIPS 200**, Minimum Security Requirements for Federal Information and Information Systems, 2006 March
- **FIPS 199**, Standards for Security Categorization of Federal Information and Information Systems, February 2004

## Other Mandates/Standards

- **OMB Mandates** (specifically M-06 and M-07)
- **Presidential Directives**
- **GSA Facility Standards**
- **NIST Standards and Guidelines**

One example of a large-scale initiative where the Government is leveraging SaaS in delivering functionality to its user community is Net-Centric Enterprise Services (NCES) eCollaboration, designed to serve communication requirements for the DoD at: [http://www.disa.mil/nces/product\\_lines/collaboration.html](http://www.disa.mil/nces/product_lines/collaboration.html). This was one of the first large-scale Federal Government initiatives to provide functionality to a large user population and to procure the services on a per-seat, compliant SaaS-delivery basis.

Other examples of public sector initiatives that may leverage the SaaS delivery model include the Presidential Directives, specifically the Lines of Business (LOB) designed to foster efficiencies, improvements and cost savings throughout the Federal Agency community.

The goals of Federal Agency LOBs are to identify opportunities to reduce the cost of government and improve services to citizens through business performance improvements. Federal Agency LOBs accounted for approximately \$20 billion in U.S. government-budgeted spending in 2007. A key delivery and support model in achieving LOB objectives are shared services – namely common services that support multiple Agency requirements. This shared services model is consistent with SaaS in many respects – with common goals to reduce cost and improve service delivery.



State and Local Government organizations are also seeking the benefits of SaaS. For example, several years ago in Fairfield County, Ohio, and Arlington County, VA, the respective economic development agencies instituted their own SaaS experiments, each using the hosted software environment for similar purposes. In Fairfield County, SaaS CRM is being used to conduct online surveys of local businesses, while in Arlington County a SaaS CRM application exists as well as an Oracle ERP solution. Along with the improved delivery and cost models of SaaS, these government organizations are paying particular attention to the security and compliance elements to protect their own citizen or internal government information.

As Government organizations' interest and inquiries regarding SaaS increase, software companies who are developing SaaS platforms are realizing that there is likely a significant gap within their current delivery operating assumptions and their compatibility with their Government customers' standards and requirements. Details of these areas are described later within this white paper; however, for those software companies that have delivered SaaS for the public sector or desire to do so, the solution infrastructure and application delivery need to be designed with the Government's current (as well as likely future) requirements and standards in mind. Some of these requirements include FISMA, DIACAP, OMB mandates, Presidential Directives, Energy Efficiency Standards, and other individual Agency-defined managed delivery requirements.

The good news for software companies is that if they can achieve a Government-compliant SaaS delivery model – with the appropriate visibility, security, control and accountability parameters – it will not only present a differentiating value proposition for the public sector, but offer a more mature and accountable framework that can be leveraged within the commercial sector as well.

# Key Technical Differences and Requirements in Delivering SaaS to Government Customers

Software/SaaS companies and most managed hosting companies are not strong in Government-compliant delivery. It is foreign in many respects, and demands specialization to execute successfully. This section highlights three key technical areas to be considered for Government-compliant SaaS offerings: IT infrastructure, multi-tenancy, data security, and integration with third party systems.

## IT Infrastructure

Commercial-grade SaaS achieves its compelling cost and service efficiencies via a shared services model with limited IT architecture boundaries, and is heavily rooted in that technological assumption. The delivery emphasis is primarily on high-availability and other elements that can be managed internally, with minimal visibility provided to the end customers on how these outcomes are achieved. Moreover, given that the public sector is rarely (if ever) the primary target customer for these SaaS companies, Government compliance criteria are neither part of the infrastructure design nor defined within the Service Level Agreements (SLAs).

With conventional (or commercial) SaaS, architectural emphasis tends to be much more on the end result, rather than the means to that end. This approach poses a problem for Government Agency decision makers who must maintain an audit trail and security accountability at all times. They must know who touches each machine, what they accessed and why. For that reason the commercial-grade SaaS model falls apart for Government organizations. This auditability of system and support activity must not only be part of the architectural design, but also be reportable per various Government agencies' requirements.

Each of the major infrastructure and delivery elements that comprise a SaaS solution has important considerations regarding how the Government traditionally implements these solutions today, and what would be acceptable (or preferred) delivery architecture for a Government compliant SaaS offering.

With conventional (or commercial) SaaS, architectural emphasis tends to be much more on the end result, rather than the means to that end. This approach poses a problem for Government Agency decision makers who must maintain an audit trail and security accountability at all times.

As the diagram below illustrates, infrastructure solution elements that comprise SaaS delivery needs to be examined in deploying a Government-compliant SaaS offering. This type of specialized infrastructure management is rarely a core competency of software companies. As such, SaaS providers looking to make (or sustain) a tangible and credible push into the public sector may elect to seek partnerships with system integrators and niche hosting providers who have extensive expertise in this area of Government-compliant infrastructure delivery.

	<b>Traditional Model for Software Deployment and Support for Government Agencies</b>	<b>Government-Compliant SaaS Delivery Model for Government Agencies</b>	<b>Without a Government-Compliant SaaS Offering or Delivery Model, Challenges for Software Companies Include:</b>
<b>Facility</b>	Implemented on-premises within Government facility	Implemented within a certified and accredited facility built to Government standards (FISMA, etc.)	Non-compliant commercial-grade datacenter facilities that do not meet stringent security standards assume greater risks and exposures
<b>Infrastructure</b>	Deployed on dedicated Agency hardware (network, servers & storage)	Deployed on dedicated Agency hardware (network, servers & storage)	Shared SaaS infrastructure and application management platforms not conducive to individual Agency requirements and standards
<b>Staff/Personnel</b>	Administration and support provided by Agency staff or dedicated contractor personnel (FTEs)	Cleared or clearable U.S. citizens; Can be outsourced to a compliant infrastructure provider; application support personnel (via SW company) also need to be addressed	Shared SaaS support personnel likely not approved to access or manage Agency data, systems or applications
<b>Policy/Procedures</b>	Developed on a system-by-system basis for SLAs, certification & accreditation and other objectives	Baseline compliant policies and procedures developed once, and can be leveraged by multiple Government organizations	Government-compliant procedures not part of commercial SaaS delivery model. Unlikely to pass security audits or other related scrutiny

## Multi-Tenancy

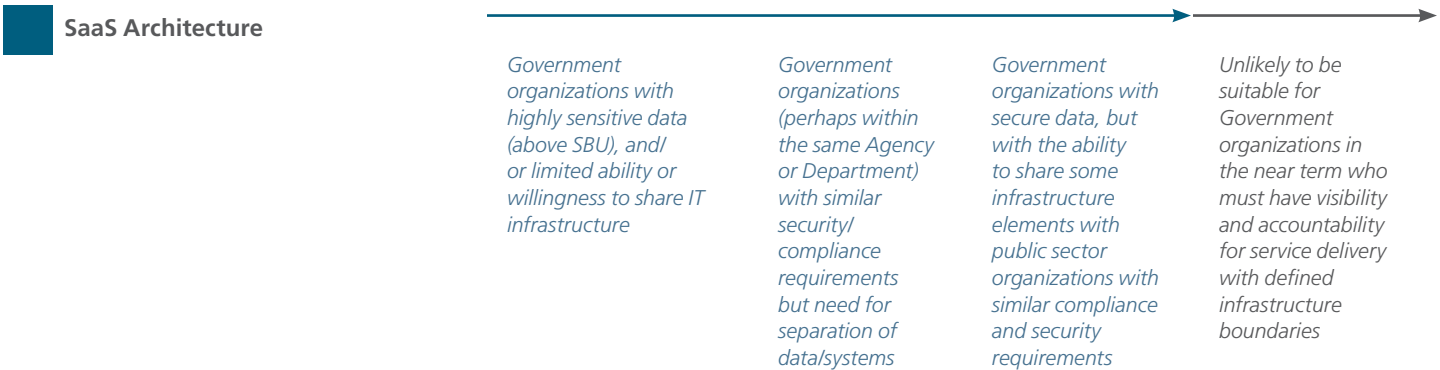
At the heart of the SaaS technical architecture is an element called multi-tenancy. Multi-tenancy refers to the SaaS IT architecture where certain elements of the architecture and/or instances of the application are shared and designed to support multiple client organizations (tenants). This architecture principle has different variations and extents to which it is deployed, but the fundamental assumption of multi-tenancy is to leverage a consolidated infrastructure and application management framework to achieve deployment economies of scale, resulting in cost savings that can be extended to SaaS customers.

Multi-tenancy is key to achieving SaaS operating model success, but requires specific treatment in order to conform to the compliance and other regulations required by the public sector. Moreover, multi-tenancy does not have a uniform or fixed architecture definition. Rather, there are a range of solution design possibilities that can be implemented to leverage more or less of the shared infrastructure, depending on the application architecture and security requirements of a given Government organization. Moreover, if an environment is designed to support multiple organizations, the multi-tenant architecture needs to satisfy the highest water mark for security and compliance for all of the Government customers that will utilize a given SaaS environment. Simply put, there are multiple and variables and scenarios to consider.

The diagram below is a high-level illustration of different architecture and multi-tenancy options that can be considered for Government-compliant SaaS environments:

## Mapping of Government Hosted Application Requirements and Proposed SaaS Architecture Approaches

	Managed Hosting Service	Isolated Tenancy	Shared Execution	Multi-tenant/ Single Version	Multi-tenant/ Multiversion
Application Execution Infrastructure	Dedicated	Dedicated	Shared	Shared	Shared
Application Versioning	Multiple	Single	Single	Single	Multiple
Data (& other Infrastructure Separation)	Physical	Physical	Physical	Logical	Logical



*\*This 4x6 (top portion) grid from a recent Gartner SaaS report*

## Data and System Security

A topic related to multi-tenancy, is how data is protected, segregated or processed within a SaaS-hosted environment. It is assumed that software firms or other SaaS-solution providers will consider overall security of the hosted solutions, however, for Government customers this requirement takes on an enhanced definition as data or applications are classified into different security levels. Depending on the level of desired availability, security or integrity of a given application, an accompanying set of delivery and compliance criteria will result that must be followed. Co-mingling of data within the same disks or devices introduces greater security or compliance risk, and specific architecture modifications must be delivered to achieve and maintain a Government-compliant SaaS offering.

## Integration with Existing Systems, Processes, & Procedures

Applications deployed in a SaaS model for Government organizations will likely need to interface with existing systems, and be a seamless – yet integrated – part of a Government's IT infrastructure. Although it would certainly be easier to deploy, SaaS applications will not likely function as an island. Agency-wide support systems and personnel such as help desk/trouble ticketing, security and information assurance, program management offices (PMO), contracting personnel and others will need to be considered regarding the SaaS environment to ensure proper interface with each Government organization's requirements. Sometimes this might require simple access to an existing SaaS information portal, while other requirements might necessitate custom development via automated interfaces/APIs, while still others may be satisfied with a manual process or information capture that is forwarded to the requesting Government organization. Regardless, in these early stages of SaaS consideration and adoption, it is a reasonable assumption that some custom effort may be required to conform to existing Government systems, and their associated policies, procedures and regulations.

# Key Business Differences and Requirements in Delivering SaaS to Government Customers

Given the still maturing adoption of SaaS within the Government space, the business trends are a bit less mature than the technical and architecture considerations. However, some patterns are emerging to be factors for SaaS companies pertaining to their business structure and pricing model. We have described a subset of business considerations within this section.

## Asset Ownership & Control

Government organizations have enjoyed a long history of owning their own equipment and IT infrastructure. Understandably, there is a comfort level, autonomy and familiarity with being able to touch and control that which one owns. SaaS in its purest form would require change in this position. That said, SaaS providers would be well served to explore alternatives such as Government-furnished equipment (GFE), and hybrid ownership arrangements for certain situations. These scenarios would almost certainly impact technical architecture assumptions such as multi-tenancy, and likely would limit the extent of cost savings that can be realized. But this may be a preferred compromise for both SaaS provider and Government entity alike to enable Government organizations to utilize SaaS in a more acceptable and controlled manner. This position might also address issues surrounding termination of agreements and subsequent rights to assets and information (addressed further within this section).

## Revenue/Pricing Model

With respect to pricing, SaaS is generally associated with per-seat models. That is, customers can activate the managed service on an individual user basis (usually per a baseline service level, with added features and functionality options that carry incremental costs) and the procuring organization would be billed on a usage (number of users) basis. "Pay only for what you use" and other compelling marketing positioning speak to the attractiveness of this model. Government procurement and contracting organizations, however, may not be structured to accommodate or work within this variable structure. Many contracts are fixed price, and procurement processes may not be able to easily support varying user counts month to month. As such, alternatives such as pricing for "not-to-exceed" user tiers or Enterprise licensing models should be considered and offered. Additionally, unplanned price increases may not be possible within a contract term given certain procurement limitations of Government organizations.

A related consideration pertains to Government organization budgets, and from what bucket of money can an Agency consider funding a SaaS application? Is it hardware, software or service? A capital or operating expense? Sales and product positioning will be important to ensure that the Government organization understands how to account for SaaS spend within their existing budget structure. 10 of 14 Regarding revenue, SaaS introduces an interesting dynamic for software companies in that (especially with per-seat pricing models), not only does the application need to be sold to generate revenue – but now it likely needs to be activated and utilized by the Government users. Depending on the Government organization, this might be easier sold than done. Selling through the point of user activation/utilization will be an important consideration if revenues are to be realized as projected by the SaaS provider. "Shelfware" was a convenient (albeit not preferred)

outcome for many software companies and their revenue plans per their Government customers. SaaS will likely change priorities of how software is sold and how subsequent revenue is recognized.

## Contract Termination and Service Assurance

For Federal Agencies, Federal Acquisition Regulations (FAR) permit an Agency to terminate an agreement under certain conditions, and for any/all Government data (and property) to be removed from a provider's systems and returned to the Government. Similar provisions exist within State and Local contracts. This requirement poses an intriguing set of considerations in SaaS delivery, and providers should be prepared technically, as well as contractually to support this requirement. For example, at the end of a service agreement, SaaS solution providers must permit and enable data exporting/migration from the hosted environment to the Government's designated infrastructure – a position not conventionally supported by SaaS providers.

An additional consideration is Service Assurance, particularly for Government application functionality that is deemed critical to health and welfare, security, or other national or civic importance. Unlike termination of a commercial customer, the nature of certain government applications or functionality may necessitate migration assistance or service assurance until such time as an alternate capability can be secured. Most often, these terms and conditions would be captured within the accompanying managed services agreements.

## Staffing and Personnel

Due to the secure and compliant nature of certain Government applications, support personnel may be required to be U.S. citizens, and/or have background checks that certify that they are free from criminal convictions, bankruptcies, or other potentially malevolent influences. Even if not required, software companies and other SaaS providers would be well served to adopt this position (internally or with their delivery partners) to help differentiate their offering from non-compliant commercial-grade providers who are competing within the public sector marketplace. Company Ownership & Localized Presence For many Government organizations, there is a requirement or at least a preference for a vendor's company ownership to be free from foreign ownership, influence or investment. For State or Local Governments, there may be a partiality towards hosting facilities or other personnel/support locations being situated in the Government's jurisdiction. Some Government Agencies go further, and require all work to be performed by U.S. citizens. These and related factors should be considered regarding the SaaS delivery facilities, company ownership structure and overall operating model.

## Past Performance/Certification & Accreditation

Government organizations will be reluctant to advance conversations re: SaaS unless the vendor can provide evidence it has obtained all security certifications required to purchase and deploy the service. Additionally, as Government organizations are risk-averse by nature, having strong current or past performance with similar or related organizations that are also SaaS customers is certainly recommended. If a software company does not have these relationships or past performance, then partnering with (infrastructure) companies who do is the suggested alternative.

## Benefits of a Federally-Compliant Infrastructure Partner

Choosing the right solution partner that is experienced with the various business and technical-level considerations of Government-compliant infrastructure delivery can yield significant benefits to software companies targeting the public sector. Examples of advantages that software/SaaS solution companies can realize include:

**REDUCE OVERALL RISK** – Issues ranging from implementation delays, required solution architecture changes, to hard stops that prevent “go-live” exist within the Government space and can be mitigated through experience and awareness of compliance and security-driven requirements. Create differentiation – The public sector is just now seriously considering SaaS solution alternatives. Early market movers will have a distinguishing advantage over their competition selling to the public sector if they have a relevant and compliant offering that meets or exceeds Government requirements.

**REDUCE COST** – Partnering with a provider that specializes in delivering Government-compliant infrastructure elements (facility, network, servers and data) will lower the overall delivery cost of a SaaS offering compared to reactively addressing issues that may arise. Distractions or delays associated with “learning” the Government space could be quite expensive in the long run.

**FASTER TIME TO MARKET** – Leveraging an existing and proven capability can shorten product development cycles by months or years. Accelerating the solution roadmap for a relevant public sector offering through effective partnership is a sensible direction for any SaaS software company or solution provider to pursue.

**FOCUS ON CORE COMPETENCIES** – Software companies are creative organizations by nature – with core competences and values around developing features and functionality within their products. Their organizational DNA is not necessarily consistent with the operations and maintenance (O&M) excellence required for SaaS delivery to keep applications highly-available and compliant for customers. To less experienced software companies, this O&M component may seem to be a simple extension of their core expertise. But as many organizations discover, managing infrastructure in a cost effective, efficient and scalable way is a business unto itself. Application-related elements and infrastructure management competencies are separate and distinct areas that require specific attention, investment, and discipline to succeed – a success that is best achieved through effective partnership.

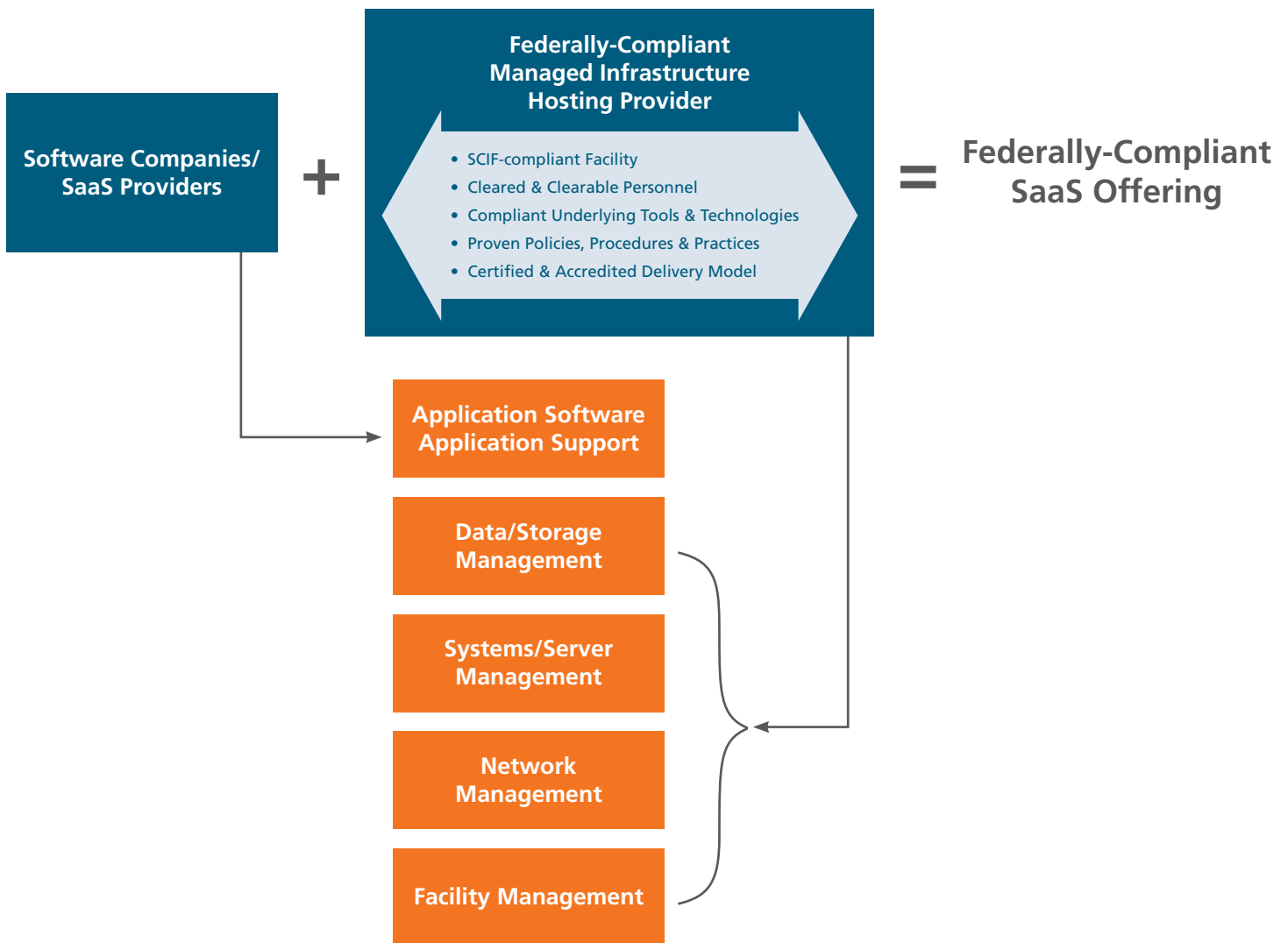
---

Choosing the right solution partner that is experienced with the various business and technical-level considerations of Government-compliant infrastructure delivery can yield significant benefits to software companies targeting the public sector.

---

**OPTIMIZE OFFERINGS FOR SPECIFIC CUSTOMERS/REQUIREMENTS** – The public sector’s approach towards SaaS is still maturing, and aside from some early adopters, the bulk of Government applications still reside on premise. As this transition to SaaS evolves, inevitably there will be organization-specific requirements or parameters that must be met in order to secure certain Government Agencies as customers. From individualized security requirements, specific reports that need to be generated, or integration with existing or legacy systems - one solution size certainly will not fit all. For these situations, having a partner who can provide flexibility within the SaaS solution model to accommodate these requirements will be invaluable to an effective go-to-market strategy.

## Federally-Compliant SaaS/Hosted Infrastructure & Application Services



# Recommendations for SaaS Providers that Target Public Sector Organizations

Based on Carpathia Hosting's experience and specialization in deploying and managing infrastructure for public sector organizations – many supporting SaaS delivery – there are a handful of actions that have proven successful in supporting applications for a multitude of Government organizations:

## Understand your Target Market and Design Your SaaS Solution Accordingly

As stated earlier within this paper, the Government market is different. There are even substantial differences across Agencies within the Federal, State and Local Government markets. Requirements these Government organizations have in the areas of security, compliance, performance-based delivery, and SLAs (to name a few) will certainly impact technical and business operating assumptions that SaaS providers must meet in order to secure these customers. In some cases, this market might necessitate standing up dedicated infrastructure or personnel, or a change in a SaaS organizations' cost/revenue model assumptions. Modifications relative to commercial SaaS delivery models are inevitable, and need to be embraced rather than resisted (or ignored).

## Take Measured Steps

SaaS is a relatively new model in the scope of information technology delivery. Compound this with an even more neophyte adoption and use of SaaS within Government organizations, and a strong case can be made regarding the value of a deliberate and measured approach to the public sector market. We recommend strong dialogue and communication between providers and customer. Ask many questions internally and of your customers regarding their expectations and requirements. Involve your customers as implementation partners. Consider beta deployments. And ensure that you capture and leverage the valuable learning you acquire along the way. Before long, SaaS providers can achieve a strong base of Government customers that can be leveraged into the broader public sector market position.

## Partner with Companies Who Complement Your Company and Improve Go-to-Market Position

The surest way for software companies to make inroads into the public sector is to identify an infrastructure partner capable of delivering SaaS-based software in a government-compliant way. This infrastructure partner should provide secure, robust IT infrastructure management and hosting services specifically designed for organizations that must maintain a stringent security posture and comply with a wide range of IT security regulations, including FISMA, DIACAP, Sarbanes-Oxley and HIPAA. With the compliant infrastructure addressed, a SaaS-provider's attention can be focused on the application detail and support, to ensure that these elements can also pass Government compliance scrutiny. The right solution partner team addresses both the infrastructure and application support requirements to establish a go-to-market position that assures customer acquisition, and offers a more scalable foundation for growth.

## Conclusion

At the SaaS for Government conference held in early 2008, Karen Evans, administrator of the OMB's Office of Electronic Government and Information Technology, further positioned herself as a SaaS advocate in relaying the key benefits. "Our track record is clear – we are not very good at delivering our own software in the time frame set," adding, "We can't continue to maintain all of the things we have. We have to start shutting down some of our legacy systems." To that point, top government officials are advocating the use of SaaS. Karen Evans, administrator at the Office of Management and Budget, has suggested that it's time for the government to embrace more service-oriented software models. The good news for vendors is that champions like Evans will continue to extol the virtues of SaaS and advocate broader adoption. The challenge associated with this market opportunity is to address the various concerns a Government Agency decision maker might have in how the software meets compliance and security obligations.

*Footnotes: \* - IDC, "Worldwide Software Business Strategies 2008 Top 10 Predictions," Doc#210334, January 2008).*

Carpathia Hosting is a leading provider of managed hosting services, delivering secure, reliable and compliant IT infrastructure and management for some of the world's most demanding enterprises and federal agencies. Founded in 2003, Carpathia Hosting is a growing, profitable business run by a seasoned management team with deep experience in delivering enterprise hosting solutions including colocation, managed services and cloud computing. Carpathia's suite of services is designed for organizations seeking scalable, secure, robust and enterprise-grade hosting solutions that can be quickly provisioned or tailored to meet unique requirements. Backed by its E3 Promise, Carpathia Hosting consistently delivers an experience that exceeds customers' expectations. Carpathia Hosting qualifies as a small business. Contact Carpathia Hosting at 1.888.200.9494, or visit [www.carpathiahosting.com](http://www.carpathiahosting.com) for more information.

CORPORATE: 43480 Yukon Drive, Suite 200 Ashburn, Virginia 20147 Voice: 1.703.840.3900 Toll Free: 1.888.200.9494 Fax: 1.703.997.5577

References to other products are made to show compatibility. All companies and/or products mentioned in this document are registered or trademarked by their respective organizations. The inclusion of third party products does not imply endorsement by these parties, unless otherwise noted.