



Cloud Computing Security Considerations and Recommendations

Usage Scenario: Software as a Service (SaaS) Electronic Mail

This paper provides an industry perspective on the security risks and unique challenges to cloud computing. The purpose of the paper is to identify solutions and best practices which consumers of cloud services and the providers of cloud services may consider to overcome these potential barriers to adoption to enable the Federal Government to realize the benefits of cloud computing to achieve missions, reduce costs and increase sharing of resources.

February 18, 2011

Prepared By:



Cloud Computing Security Working Group

Cloud Computing Security Considerations and Best Practices for SaaS Email

Executive Summary

Cloud computing has risen to be one of the key IT infrastructure imperatives and opportunities to achieve efficiency throughout the Federal government for 2011 (and beyond). Many agency personnel are in a learning mode regarding the details of what makes for a successful and secure cloud computing implementation. The General Services Administration (GSA), Federal Cloud Computing Initiative (FCCI), contacted ACT-IAC seeking assistance with Software as a Service (SaaS), Electronic Mail security challenges. The ACT-IAC Cloud Computing Cross Shared Interest Group was engaged, a working group formed and the attached paper developed. The working group was composed of industry professionals from IAC member companies, representing diversity of the government IT industry. This paper identifies some of the unique security risks and challenges of SaaS Email as well as presents best practices and solutions in the context of usage scenarios that most agency personnel can relate. This white paper also incorporated new Federal security guidance, FedRAMP, and provides perspectives and recommendations on how government can approach and secure their respective cloud-based implementations for email.

Acknowledgements

Contributors

ACT-IAC would like to thank the following members that contributed significantly to the development of this paper: Jim Graham, SecureIT; Michael Donovan, HP; Seth Finkel, FedVision; Habib Nasibdar, USmax Corporation; Josh Rosenthol, NetWitness; Joe Houle, AT&T; and Kevin McDonald, ICF.

ACT-IAC would also like to recognize other members of the Cloud Computing Shared Interest Group that participated in review and comment on this paper: Billy Baker, AT&T; Scott Dowell, CSC; Terry Miller, CSC; Patrick Cronin, CGI-Federal; Mike Rohde, SecureInfo; Bryan Ward, Serco; and Vic Winkler, Booz Allen Hamilton.

The Cloud Computing Security Working Group would also like to acknowledge and thank Katie Lewin and Doug Hansen of the GSA FCCI program office for their input and guidance that assisted the working group members to identify and understand the unique challenges of the program.

Cover Page Photo courtesy of Sebastian Brosen.

Cloud Computing Security Considerations and Best Practices for SaaS Email

About ACT-IAC

The American Council for Technology (ACT) is a non-profit educational organization established in 1979 to assist government in acquiring and using information technology resources effectively. In 1989 ACT established the Industry Advisory Council (IAC) to bring industry and government executives together to collaborate on IT issues of interest to the government. In 1997 ACT established the Intergovernmental Advisory Board (IAB) to foster communication and collaboration between IT executives at all levels of federal service – Federal, state, local and tribal governments.

The American Council for Technology, in cooperation with the Industry Advisory Council and Intergovernmental Advisory Board, is a unique, public-private partnership dedicated to helping government use technology to serve the public. The purposes of the organization are to communicate, educate, inform and collaborate. ACT also works to promote the profession of public IT management. ACT and IAC offer a wide range of programs to accomplish these purposes. ACT and IAC welcome the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of information technology.

For further information, contact the American Council for Technology and Industry Advisory Council at (703) 208-4800 or www.actgov.org.

Disclaimer

This document has been prepared to provide information regarding a specific issue. This document does not – and is not intended to – endorse or recommend any specific technology, product, or vendor. The views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable information in this report. However, ACT-IAC assumes no responsibility for consequences resulting from the use of the information herein.

Copyright

©American Council for Technology, 2011. This document may be quoted, reproduced and/or distributed without permission provided that credit is given to the American Council for Technology and Industry Advisory Council.

Table of Contents

1	Introduction	1
2	Solution Context - Ownership of Controls in diverse Provider/Consumer Relationships.....	2
3	Usage Scenario: Shared Cloud Mail Service.....	3
3.1	Description	3
3.2	G2CM: Government Access to Certified Provider (Hybrid)	5
3.3	Considerations for Solutions that involve 3 rd Party Non-Certified Service Providers.....	6
4	Challenge Areas and Risks Unique to Cloud Computing – Summary.....	7
4.1	Network Security and Trusted Internet Connection (TIC)	8
4.2	Multi-Tenancy and Boundary Control.....	11
4.3	Information Management	12
4.4	Identity and Access Control Management.....	15
5	FedRAMP Security Controls	17
6	FedRAMP-based Analysis; Security Considerations.....	17
6.1	G2CM Assumption: Government Access to Certified Provider (Hybrid)	18
6.2	C2CM: Controlled Access to Certified Provider (Hybrid)	27
7	References	31
8	Appendix A: Risks Specific to Cloud Computing and Recommended Mitigations/Solutions.....	32
8.1	Trusted Internet Connection (TIC) Considerations	32
8.2	Boundary Constraints and Multi-Tenancy	34
8.3	Identity Management and Access Control.....	40
8.4	Data Security, Ownership and Retention.....	41
8.5	Incident Response and Forensics.....	43
8.6	Governance, Security Authorization and Continuous Monitoring	46
8.7	Solutions and Best Practices	51

List of Tables and Figures

Table 1: Access/Facility Pairs Describe Deployment Situations Anticipated by Federal Agencies	3
Figure 1: Email Software as a Service (SaaS) Notional Architecture.....	5
Figure 2: Use of Non-Certified Service in SaaS Email Solution	6
Figure 3: Boundary Considerations in Multi-Tenant Environments	11

1 INTRODUCTION

In response to a request from the General Services Administration (GSA), Federal Cloud Computing Initiative (FCCI), the American Council for Technology (ACT) Industry Advisory Council (IAC), assembled a working group comprised of experienced cybersecurity, cloud computing and risk management professionals from IAC member companies. Formed from the Cloud Computing Shared Interest Group, the charter of this working group was to provide the GSA FCCI program industry perspective on the security risks unique challenges to cloud computing identifying solutions and best practices which organizations may consider to overcome these potential barriers to adoption. The working group was composed of industry professionals from IAC member companies, representing diversity of the government IT industry. This working group was empanelled under operating principles and guidelines as established by the IAC Board of Directors and in accordance with the IAC Code of Conduct.

As there are numerous business cases and cloud computing deployment models and associated solutions available today and continuing to emerge, the working group, through collaboration with the GSA FCCI program office, selected the Software as a Services (SaaS) deployment model for the business case of Electronic Mail (email) on which to analyze and provide recommendations.

The paper is organized as follows:

Section 2: Introduction of the context/scenarios we are addressing within this white paper, and also a summary of the different providers and consumers of cloud-based solutions and services.

Section 3: Usage Scenario: Shared Cloud Mail Service. The working group analyzed two Access/Facility pairs in the context of SaaS Email identifying control implementation ownership considerations by the Provider, Consumer and the Boundary

Section 4: Challenge Areas / Risks Unique to Cloud Computing. The working group identified the unique challenge areas, threats and associated risks associated with SaaS Email in the following domains:

- Network Security and Trusted Internet Connection (TIC)
- Multi-Tenancy and Boundary Control
- Information Management
- Identity and Access Control Management

Section 5: The draft version of FedRAMP¹ posted for comment in November 2010 was examined to support the development of this paper. Refer to GSA or CIO.gov for the latest information on the FedRAMP program, security controls and security authorization process.

Section 6: Provides examination of the NIST SP 800-53 security controls applicable to the use case (SaaS Email). The working group identified and analyzed considerations for both the G2CM Assumption:

¹ <http://www.cio.gov/pages.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP>

Cloud Computing Security Considerations and Best Practices for SaaS Email

Government Access to Certified Provider (Hybrid) and C2CM: Controlled Access to Certified Provider (Hybrid). The focus of the examination was on FedRAMP security controls specified for a Moderate impact system that present unique challenges. For each challenge area, the paper provides example solutions of control implementation along with suggested control ownership.

Section 7: References per the content of this white paper are listed with their respective sources

Appendix A : The working group captured considerations for within a set of detailed matrices regarding identified elements that would need to be addressed with respect to email software as a service delivery including:

- Boundary Constraints and Multi-Tenancy
- Identity Management and Access Control
- Data Security, Ownership and Retention
- Incident Response and Forensics
- Governance, Security Authorization and Continuous Monitoring
- Application Security (*not addressed in this paper due to insufficient resources*)
- Operational Support Systems (*not addressed in this paper due to insufficient resources*)
- Disaster Recovery / Contingency (*not addressed in this paper due to insufficient resources*)

2 SOLUTION CONTEXT - OWNERSHIP OF CONTROLS IN DIVERSE PROVIDER/CONSUMER RELATIONSHIPS

Aside from the existing definitions for cloud computing already defined by NIST, the working group determined the need to expand on these definitions to support the objective of this paper. The following terms are used within the context of this paper to aid in the interpretation of requirements and to assist in conveying differences in how security controls apply and must be implemented depending on the who accesses the information, the locations which the information is stored, and the level of security certification of business partners. Refer to NIST guidance for definitions of Cloud Computing Models and associated characteristics.

Term	Definition
Government Access	Access using a government controlled device from an authenticated user
Controlled Access	Access from a device which may not be controlled by the government from an approved authenticated user
Public Access	Access from a device which may not be controlled by the government by an unauthenticated user
Dedicated Government Facility	Single-tenant dedicated data and processing environment hosted

Cloud Computing Security Considerations and Best Practices for SaaS Email

Term	Definition
	on government controlled premises
Shared Government Facility	Multi-tenant, government community, shared data and processing environment on government controlled premises
Certified Provider Government	Multi-tenant, government community, shared data and processing environment on commercial premises, certified via FedRAMP
Certified Provider Hybrid	Multi-tenant, govt and non-govt customers, shared data and processing environment on commercial premises, certified via FedRAMP
Public	Multi-tenant, govt and non govt customers, shared data and processing environment on commercial premises, industry best practices and associated audit (e.g. SAS 70)

The table below depicts a representation of the different combinations of Access / Facility pairs which government agency customers may encounter in obtaining internally provided and externally provided cloud computing solutions. Through collaboration with the GSA FCCI program office, the working group determined that of the pairs identified in this table those shaded in red presented the situations most in demand and thus became the focus of the working group’s analysis.

Table 1: Access/Facility Pairs Describe Deployment Situations Anticipated by Federal Agencies

Access Type	Facility / Compute System Control				
	Dedicated Government	Shared Government	Certified Provider, Govt	Certified Provider, Hybrid	Public Provider
Government	G2DG	G2SG	G2CP	G2CM	G2PP
Controlled	C2DG	C2SG	C2CP	C2CM	C2PP
Public	P2DG	P2SG	P2CP	P2CM	P2PP

3 USAGE SCENARIO: SHARED CLOUD MAIL SERVICE

3.1 Description

Provider

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

- Commercial Mail Provider whose data center facility has been certified as compliant to a FISMA Moderate level.

Consumer

- The mail service is offered to government employees across several agencies within a department who form the service user base
- The government users are assumed to access the mail service from government issued desktops, PDA's and mobile laptops. No access in this scenario from non-government devices
- Consumers may access mail service through client/server (Outlook client/Exchange) or web-based method.
- The mail service may also be bundled with an office suite of applications such as word processing, spreadsheet and presentation.

Information Categories

- The mail service will contain both restricted and unrestricted data
- Restricted data: FOUO, PII, Competition Sensitive, Supplier Proprietary (examples)
- Unrestricted data: messages received or sent to broad distributions (public), personal communications, advertisements, etc
- The mail service will store both mail messages and attachments of various types
- Some mail messages will meet the criteria for records and are subject to retention schedules
- Some mail may be subject to legal discovery and hold actions

Assumptions

- Some users will use the public cloud, some a private internal mail service and some may use both

The figure below depicts a high level depiction of typical components of an email service in the context of a described usage scenario above via a cloud computing model and the access/facility types expressed in this paper.

Cloud Computing Security Considerations and Best Practices for SaaS Email

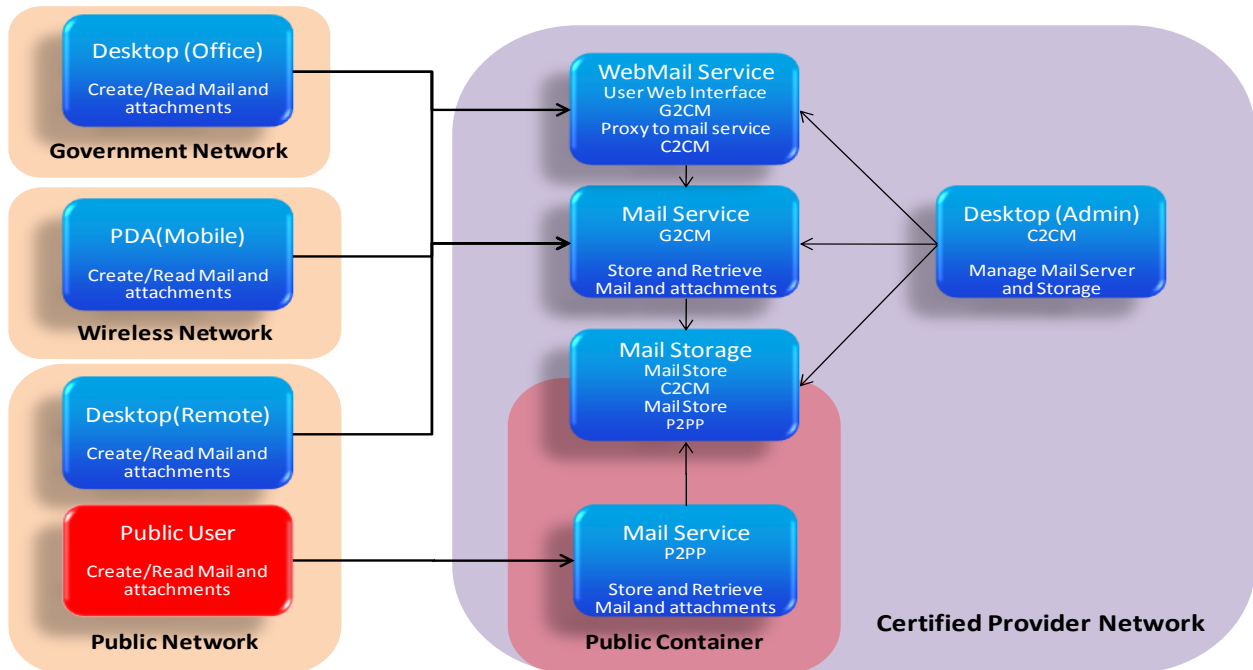


Figure 1: Email Software as a Service (SaaS) Notional Architecture

The Email solution will be constructed in different ways by vendors ranging from a single provider to multiple provider integrated solutions. The manner in which the solution provider architects the components of its SaaS email solution will determine the security controls and the type and form of agreements with business partners to ensure appropriate security requirements/controls are specified along with the necessary monitoring to support FedRAMP continuous monitoring and reporting requirements.

3.2 G2CM: Government Access to Certified Provider (Hybrid)

In this access/facility pair, an authenticated Government User/Device consumes a service provided by a certified provider in a hybrid cloud model.

Provider

- Commercial Provider whose data center facility has been certified as compliant to a FISMA Moderate level.

Consumer

- Government employees across several agencies within a department who form a service user base. The government users are assumed to access the service from government issued desktops, PDA's and mobile laptops. No access assumed from non-government controlled devices

Information Categories

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

- The service will contain both restricted and unrestricted data. The service will store documents or data of various types. Some data will meet the criteria for records and are subject to retention schedules. Some data may be subject to legal discovery and hold actions

Assumptions

- Some users in the user base will use the public cloud, some a private internal service and some may use both (hybrid)

3.3 Considerations for Solutions that involve 3rd Party Non-Certified Service Providers

Solution providers may elect to design solutions that leverage internal services or 3rd party providers. If the 3rd party provider's service is not FedRAMP certified at or above the necessary FIPS PUB 199 security impact level, the SaaS Email solution provider will need to provide information to support risk based decisions.

Example: SaaS Email solution provider obtains storage service from a 3rd party which is not FedRAMP certified.

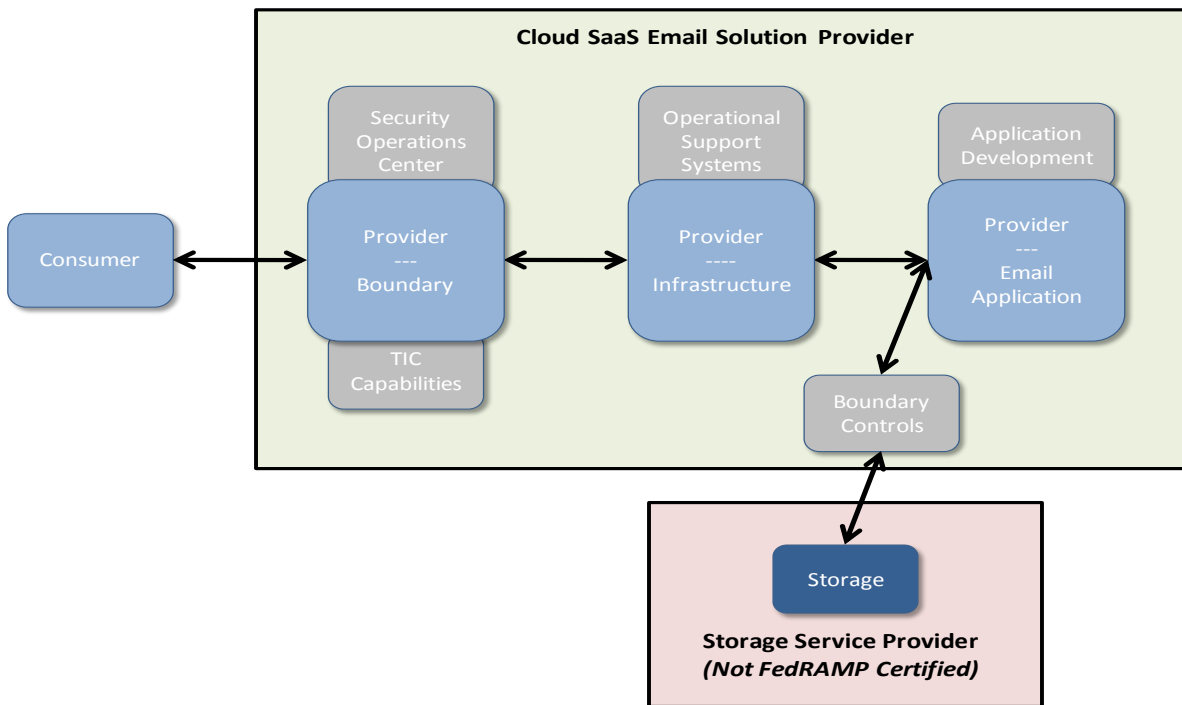


Figure 2: Use of Non-Certified Service in SaaS Email Solution

Cloud Computing Security Considerations and Best Practices for SaaS Email

Special consideration should be given to the following areas:

Maintenance

- Understanding of (and possible audit of) providers' delivery partners to ensure compliance with Agency requirements
- Extension of maintenance operations policies and documentation to other providers within the delivery ecosystem.

System and Communications Protection

- Understanding of (and possible audit of) providers' delivery partners to ensure compliance with Agency requirements
- Review, evaluation, and (possible) modification of TIC infrastructure/configurations to protect Agency from unauthorized access from provider set beyond the primary email service contractor
- Issue policy guidance to providers pertaining to security and compliance – particularly pertaining to restricted data.
- Network paths and controls to ensure that 2nd or third tier delivery partners will not circumvent security/filtering provided by the TIC.
- Implement network and system architecture/controls such that TIC and other security and compliance measures that have been established and certified with primary contractor/provider are assured with the extension of delivery to other outsourced partners (storage, etc.)
- Perform scheduled and unscheduled audits of external providers to ensure compliance with security measures and controls.

4 CHALLENGE AREAS AND RISKS UNIQUE TO CLOUD COMPUTING – SUMMARY

The trend toward Cloud Computing is a natural evolution in the way IT is acquired, provisioned and used to support business or mission functions. As more and more of the resources that have traditionally been provided by internal IT organizations in a custom manner to support programs become available as low cost services the need for custom built solutions diminishes. While some programs handle information that may continue to require dedicated or private cloud solutions, the use of public or hybrid cloud resources offers a level of cost savings and agility that is likely to expand their use. One specific application that is a likely candidate for cloud-based solution adoption within Federal agencies is email. As such, the working group considered email as a working reference point and application example per challenge areas and risks that are pertinent within cloud computing-based solutions.

An examination of the security risks and implementation issues associated with this movement towards the use of cloud computing resources, particularly against the existent set of controls and best practices has led to a number of conclusions and areas where discussion is warranted. In many cases, the risks and controls applied to dedicated IT resources are applicable to systems built from cloud based

Cloud Computing Security Considerations and Best Practices for SaaS Email

resources. As the use of cloud resources continues to evolve, this list of key issues is likely to evolve, particularly as tools and practices mature. A number of groups and standards bodies across industry, such as the Cloud Security Alliance, the Trusted Computing Group, The Open Group and others, are publishing work which addresses much of the detailed description of risks and their resolutions, but there are a few broad areas that we would like to present for discussion. The multi-tenant and multi-provider nature of cloud computing drives a discussion of the fluid nature of system boundaries and multi-tenancy.

- The Trusted Internet Connection (TIC) initiative presents interesting considerations when extended to cloud computing environments – particularly with content that was previously assumed to be within the Agency premise, and may move to an external provider/entity in a cloud-based solution.
- Multi-tenancy occurs at different levels and each level brings with it unique challenges.
- The distributed nature of cloud computing IT raises significant issues regarding information protection:
 - o Loss of physical control
 - o Effects of availability mitigation (multiple copies to multiple providers)
 - o Data forensic implications
- The shared nature of cloud computing solutions and the fluid nature of system boundaries raises important network implications:
 - o Content protection when data leaves internal network (including cloud provider internal network)
 - o Routing challenges (to force data to use the TIC (trombone effect))
 - o Who owns the problem (see below)
 - o Performance trade offs
- The multi-provider and shared resources inherent in composite applications raise issues related to identity and Access Management
 - o User identities
 - o Brokered Identities
 - o Device Identities
- From a cloud resource consumer perspective, a clear understanding of the internal and external provider and consumer relationships leads to a shifting responsibility for security control implementation, monitoring and compliance:
 - o who participates in the relationship shifts the responsibility for policy enforcement (i.e. govt to provider, certified provider to government, cp to public, public to government, etc.)

4.1 Network Security and Trusted Internet Connection (TIC)

The Network Security and Trusted Internet Connection (TIC) is a key element in the Federal Government's overall strategy to protect the overall network infrastructure across and within the Federal Agency community. Per the TIC Reference Architecture document (v2 DRAFT), "The overall

Cloud Computing Security Considerations and Best Practices for SaaS Email

purpose of the Trusted Internet Connection (TIC) Initiative, as outlined in OMB Memorandum M-08-05, is to optimize and standardize the security of individual external network connections currently in use by the Federal Government, to include connections to the internet. The initiative will improve the Federal Government's security posture and incident response capability through the reduction and consolidation of external connections and provide enhanced monitoring and situational awareness of external network connections.”

Per the objective of this document, ACT-IAC cloud computing security SIG representatives have examined the considerations and impact of a cloud-computing-based hosted email system with respect to the TIC, and have offered a summary of Risks and Challenge Areas Unique to Cloud Computing and Control Design to Mitigate Risks and Permit Adoption/Use of Cloud Services.

Depending on how the U.S. Government intends to leverage the Trusted Internet Connection (TIC) with cloud computing solutions, there likely would be a series of considerations to maintain the overall security posture for the Agencies – specifically the path between the TIC node(s) and the respective cloud computing providers/solutions.

At a high level, the mission and key objective of the Trusted Internet Connection program – specifically to limit the number of Internet connections within the U.S. Government – likely runs counter to the Federal Agency adoption of diverse, geographically-disparate cloud computing solutions. More specifically, the diverse set of cloud computing solution providers, technologies and geographies – most of which use the Internet as their primary method of inter-site and external communications – would likely necessitate *expansion* of the Internet ingress and egress points within the Federal government rather than contraction of those access points.

Some other TIC-related considerations:

- Are TIC connections within FedRAMP-approved providers' infrastructure being considered?
 - o If so, TIC controls and validation would need to be added to the current FedRAMP set of operations requirements. (i.e. the 50 baseline security capabilities in TIC 1.0, and the National Cyber Protection System – EINSTEIN)

- Where TIC inspection occurs and what is inspected:
 - o It may be complex for FedRAMP-approved Cloud computing providers to maintain compliance with other TIC provisions, especially if Federal data resides in different locations or can be accessed by cloud administrator personnel located in different sites. For non-FedRAMP-approved cloud computing providers, compliance would likely be unlikely to be achieved or maintained.

 - o With Agency data moving to external cloud hosting providers, the scope of TIC inspection would need to be broadened to accommodate the additional data sources, geographies, and organizations per cloud computing providers others who are transmitting sensitive Agency data. (Email would certainly fall within this data sensitivity category.)

Cloud Computing Security Considerations and Best Practices for SaaS Email

- With external cloud computing solutions supporting applications that normally reside internally within an Agency – such as email (with attachments, etc.) - there could be a shift in what are now considered “internal communications” to those that are external, thus (potentially significantly) increasing the volume of data that would need to be inspected by an Agency/TICAP TIC infrastructure. This might necessitate expansion of the number of internal Agency-approved TIC nodes or sites to ensure efficient application/ network performance.
- Additionally, as this landscape changes, on-going review will be needed as applications move to, between and from external cloud providers to ensure that the TIC is inspecting appropriate sources.
- Data classification:
- Modes of access and communication
 - Given the range of wireless devices that can access email, attention should be paid regarding users’ potential disintermediation of TIC nodes (e.g. users remotely accessing email and then internally syncing their cell phones, iPads, within the LAN infrastructure.) There are several network configuration possibilities to minimize risk, and a combination of technical and policy-based controls are advised for each Agency.

Recommended approaches:

Given the scenario that the TIC initiative and cloud computing adoption were to move forward in parallel, and then a hybrid strategy would be recommended to be engaged. One concept follows:

- Inspection of the network could occur at the Federal Agency boundary to inspect and protect the Federal Agency users and infrastructure. Particular emphasis should be placed on monitoring/inspecting inbound communications to the Agency infrastructure given the shift of previously internal applications (such as email) to external providers
- Controls would need to be implemented and maintained within the cloud computing providers to ensure that internal risks are minimized (such as data exfiltration by cloud administrators or any unauthorized users). Collaboration with the TIC program could improve the security provided by cloud providers if the signatures, patterns, keyword list and other inspection criteria could be shared. In lieu of collaboration with external cloud providers, significant emphasis on outbound content examination at federal boundaries should be considered to ensure awareness or restriction of content placed outside the federal boundary.

Other recommendations:

- Engage cloud computing providers, and bring them into the TIC fold. They could be useful in providing perspective and suggestions on how TIC (or at least comparable TIC inspection/monitoring) could be extended into the cloud computing provider infrastructure
- Cloud computing providers’ solution network design/architecture should be addressed with TIC nodes to ensure that inbound communications to the Agencies are adequately accounted for (i.e. geographic considerations if content can be dynamically served from various sites, etc.)

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

- Assuming email is outsourced to a cloud provider, TIC inspection should be strengthened at the Agency premise or TICAP provider for email specific protocols and communications (SMTP, POP3, IMAP4, etc.) and email-related communications. Moreover, regarding data sensitivity levels, email communications and attachments can easily span various data sensitivity levels depending on user controls and behavior. Emails, data or documents attached or remotely accessed using office automation tools over HTTP may need to be addressed as well, depending on whether a full document or simply HTTP data transits the boundary. These issues should be taken into account per the scope and nature of TIC inspection.
- Institute bi-directional reviews to ensure that over time, external entities’ communications to the Agencies are still active and – if not – have them removed from the TIC inspection listing

4.2 Multi-Tenancy and Boundary Control

In a classic IT system design, the infrastructure is custom designed to meet the needs of the systems it supports. This relatively tight binding between the infrastructure and system boundaries and its static nature allows the security architect and operations staff to implement system controls at infrastructure boundaries. One of the implications of moving towards cloud computing with its reliance on shared infrastructure delivered by multiple providers is the need to separate and loosely couple the infrastructure and system boundaries. (Figure 1)

A **Boundary**, for the purposes of this discussion, is the edge of a logical domain characterized by a consistent set of policies, rather than a physical construct. A cloud consumer boundary is the set of controls and operational practices that are consistently applied across all assets within the domain. A cloud provider boundary is similar in that it encompasses the set of policies governing use and operation of the provider’s resources. The relationship between them can be many to many and so a consumer is responsible for governance of their policy in a multi-provider domain, and a provider must enforce their policies in support for multiple consumers. A boundary condition is defined as the effect of information or services crossing one of these policy boundaries and the risks that must be governed when this occurs.

Multi-tenancy is the sharing of provider resources by multiple consumers. This is a relative construct. For example, from a facility perspective, all resources in the facility can be physically allocated to separate consumers, but the facility is multi-tenant (co-location is an example). From a server perspective, multi-tenancy might be

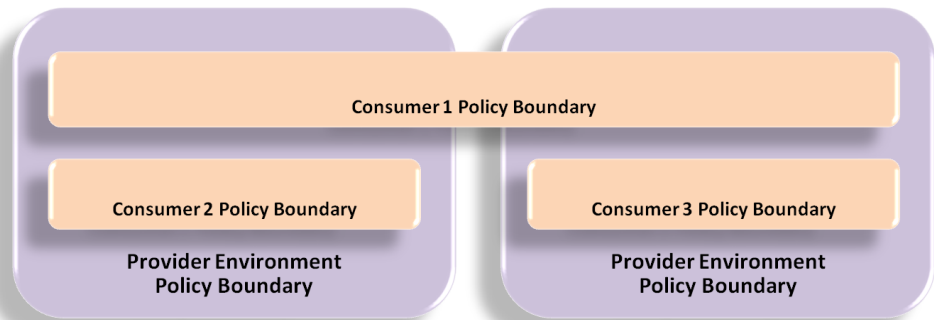


Figure 3: Boundary Considerations in Multi-Tenant Environments

Cloud Computing Security Considerations and Best Practices for SaaS Email

allocation of blades, virtual machines or shared OS images. For storage, multi-tenancy might involve dedicated volumes with a shared chassis/controller or logical volumes sharing the same physical drive. And so forth through network, user device, application and peripherals. The key concept is that a resource is multi-tenant depending on the level of infrastructure from which you view the situation.

A risk is assumed to be related to multi-tenancy if the attack surface of the resource, at the level under consideration, exists because it is shared by multiple consumers. Mitigation involves implementing separation between the tenants of the resource. The best practice for implementing separation controls is a sliding scale that reflects a degree of risk. In most cases, this is offset by an implementation cost that is generally higher for the more secure forms of separation. Examples of separation techniques might be:

- **Physical separation** provides a discrete physically separate instance of the resource.
- **Virtual Separation** provides a logically separate instance using shared physical resources.
- **Cryptographic Separation** uses encryption to separate information streams or repositories. Only consumers with the appropriate decryption key and algorithm can gain access.
- **Access Control / Permission based Separation** uses policy based controls enforced by the software system to grant access to resources.
- **Open Access** assumes no need for separation from other tenants

Physical separation is assumed to be a stronger level of enforcement than virtual or cryptographic. The scale balances risk vs. cost.

The real issue for cloud computing consumers is the need to manage a potentially complex set of overlapping boundaries and policy sets to meet the needs and obligations of the target application domain. For a capability such as messaging and collaboration, there is likely to be a hybrid set of providers, both internal and external to the government networks.

Best practices involve systems integration methodologies, compliance monitoring, risk management and the infrastructure separation approaches previously discussed to define the risk profile, implement separation, measurement of compliance and coordinate activities of suppliers to meet user needs.

4.3 Information Management

A central and seminal aspect of any IT infrastructure solution is the manner in which data is managed within the environment – from its origination, through management, retention and ultimately proper destruction or archival. Per the solution example of this white paper, email systems have various information sources that would need to be managed and protected – to include email message content, associated attachments, and arguably, some of the email addresses, distribution lists, header information such as teleconference phone numbers and locations of meetings.

According to ARMA International’s Guideline for Outsourcing Records Storage to the Cloud, “Storing data or using applications in the cloud does not relieve the organization of the responsibility for the

Cloud Computing Security Considerations and Best Practices for SaaS Email

protection or management of its data. The organization must ensure that private data, or data with a limited scope or accessibility, remain secure and that access is managed.”

Moreover, U.S. Federal Agency’s distinct requirements regarding the treatment of sensitive vs. public information adds a compartmentalized element of cloud-based services that would need to be demonstrable within any FedRAMP or other cloud solution provider.

There are many aspects of information management, and the authors of this white paper have highlighted and identified a few key areas for consideration. These include: data sovereignty, data security, and retention.

Data sovereignty is defined as the ownership, access and rights to data with respect to geographic and political boundaries, or other conditions of domain control. Per Vivek Kundra’s comments during a recent *World Economic Forum Cloud Computing Workshop November 3, 2010*. “In the cloud, data can be maintained and housed outside traditional boundaries, forcing us to confront issues regarding data sovereignty. From local governments to nation-states, laws, regulations and policies may vary regarding access to and control of data within a given set of borders.” With cloud computing architecture based on pooled resources that are not necessarily compartmentalized or geographically limited by design, ensuring that providers or solutions have sufficient parameters in place to ensure full Agency ownership, access and control of the data is of paramount importance. Solutions that are bounded geographically per where data is hosted is an important step in this direction (e.g. hosted within the United States), but wherever Agency data is not located on premise or in a single location should be contemplated per scenarios where Agency personnel must be able to have control of and access to their information. Contractual clauses within cloud service agreements should be written to address data sovereignty concerns, and – where applicable – test scenarios should be exercised to proactively ensure how the service provider would react and perform.

Data security has many components, but at a high-level protection of the data that leverages a cloud environment needs to be secured per the transport in and out of the cloud, as well as within the cloud environment. Data encryption, VPN-tunneling, are all common methods to address some of these challenges, but an Agency-specific, end-to-end analysis of a cloud computing provider’s solution to include where data originates, how it is accessed and updated, where it is stored, who has access privileges, etc. – should all be carefully scrutinized not only initially – but throughout the service relationship with the cloud computing provider(s). As many cloud computing providers leverage subcontractors for certain portions of the service, an integrated picture needs to be communicated by the contracted provider and understood by the Agency personnel. In short, the fact that the cloud solution is a “service” does not preclude the providers from demonstrating how data security is achieved, and providing evidence of their delivery model.

Regarding **data retention**, there are policy-related mandates that need to be addressed (per NARA), but there is also a financial impact to these cloud-based practices, as the total cost needs to include what information needs to be stored (and paid for) and what can safely be purged (and by whom).

Cloud Computing Security Considerations and Best Practices for SaaS Email

NARA highlights several relevant considerations and provides guidance/suggestions regarding the management of information within cloud computing environments. Per the NARA web site, a bulletin issued September 08, 2010 provides a good summary of the challenges and provides recommendations for agencies”

<http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html>:

“NARA has identified several records management challenges with cloud computing environments:

- Cloud applications may lack the capability to implement records disposition schedules, including the ability to transfer and permanently delete records or perform other records management functions. Therefore, specific service and deployment models may not meet all of the records management requirements of 36 CFR Part 1236 (formerly 36 CFR part 1234). Examples of these requirements include:
 - Maintaining records in a way that maintains their functionality and integrity throughout the records' full lifecycle
 - Maintaining links between the records and their metadata
 - Transfer of archival records to NARA or deletion of temporary records according to NARA-approved retention schedules.
- Depending on the application, cloud service providers must be made aware of the record retention requirements governing a given body of Federal records stored in one or more cloud locations. Agencies need to be able to control any proposed deletion of records pursuant to existing authorities, wherever the records may be located in the providers' cloud. Cloud service providers must also act to ensure that records are accessible so as to ensure agency responsiveness to discovery, or FOIA/Privacy Act, or other access requests.
- Various cloud architectures lack formal technical standards governing how data are stored and manipulated in cloud environments. This threatens the long-term trustworthiness and sustainability of the data.
- A lack of portability standards may result in difficulty removing records for recordkeeping requirements or complicate the transition to another environment. This could affect the ability of agencies to meet their recordkeeping responsibilities for temporary or historically valuable records being transferred to NARA.
- Agencies and cloud service providers should anticipate how continued preservation and access issues will be resolved in a contingency where the cloud service provider's business operations materially change (e.g., bankruptcy), or cease altogether.

Cloud Computing Security Considerations and Best Practices for SaaS Email

How can agencies meet their records management responsibilities?

The following are guidelines for creating standards and policies for managing an agency's records created, used, or stored in cloud computing environments:

1. Include the agency records management officer and/or staff in the planning, development, deployment, and use of cloud computing solutions.
2. Define which copy of records will be declared as the agency's record copy and manage these in accordance with 36 CFR Part 1222. Remember, the value of records in the cloud may be greater than the value of any other set because of indexing or other reasons. In such instances, this added value may require designation of the copies as records.
3. Include instructions for determining if Federal records in a cloud environment are covered under an existing records retention schedule.
4. Include instructions on how all records will be captured, managed, retained, made available to authorized users, and retention periods applied.
5. Include instructions on conducting a records analysis, developing and submitting records retention schedules to NARA for unscheduled records in a cloud environment, These instructions should include scheduling system documentation, metadata, and related records.
6. Include instructions to periodically test transfers of Federal records to other environments, including agency servers, to ensure the records remain portable.
7. Include instructions on how data will be migrated to new formats, operating systems, etc., so that records are readable throughout their entire life cycles. Include in your migration planning provisions for transferring permanent records in the cloud to NARA. An agency choosing to pre-acquisition its permanent electronic records to NARA is no longer responsible for migration except to meet its business purposes.

If an agency decides to create or join a private or community cloud, it will still need to meet records management responsibilities. The agencies may describe these responsibilities in agreements among the participating offices or agencies. If a cloud provider ceases to provide services an agency must continue to meet its records management obligations. Agencies should plan for this contingency.”

4.4 Identity and Access Control Management

While Identity and Access Control (IAC) is not unique to cloud computing, the complex relationships between providers and consumers increase the need to plan and manage access controls and identity credentials. There are a number of concepts in the IAC space that are worth a short discussion before moving on to the cloud specific considerations.

- Identity describes a unique entity, being a person or device, who may participate in a system interaction. Generally, each individual or device has a single identity.
- A persona represents an aspect or role that an identity exposes for the purposes of an interaction. For example, an individual may have many personas representing different

Cloud Computing Security Considerations and Best Practices for SaaS Email

aspects of their work or personal like. A device may have the persona of a server, a mail server, or other roles they expose within a certain type of relationship.

- A credential is an artifact that asserts some attributes about an identities persona for use in confirming or describing the attributes or role of the entity in an interaction.

Credentials are the key to interoperability in a multi-provider cloud ecosystem. The ability to share information about parties in a transaction in order to establish access rights (authentication and authorization) in a trusted context without requiring each party to have discrete credentials issued by each provider allows composite systems to function without alienating the user community. Many security experts today are promoting the use of a single credential to accomplish this, but that approach carries fairly high risks. If a single credential is assigned to an identity, then the compromise of that credential is bound to access permissions to resources for all of the personas of an identity. If however, the hierarchical relationship of identity to multiple personas to multiple credentials is maintained, then the damage caused by compromise of an individual credential is limited. Recurring use or one-time credentials can allow a user access to a system and the assertions and other information released to a provider system targeted to what is necessary for the transaction. Rather than require a user to retain knowledge of many credentials and passwords, a credential broker can issue tokens to a user for use in specific scenarios, minimizing the complexity from a user perspective.

There are a number of provider and consumer relationships that are likely to be used in combination and each may generate a slightly different set of requirements and obligations for the parties.

- G2DG relationships are likely the simplest, as they need to conform to PIV (HSPD-12) standards for credentials and the risk of using those credentials is fairly low.
- Government relationships with certified providers may vary in risk profile, but are generally thought to be risk managed through the FedRAMP security assessment and authorization process. Assertion of government credentials to certified providers is likely appropriate, although an agency may choose to use a credential broker to send an alternate trusted credential to a provider in mixed tenant environments to protect the government credential from interception.
- Certified providers accessing government resources may be issued government credentials, can establish a trust relationship with the government for use of the providers own credentials, or use the services of a credential broker to establish the identify of a user.
- Government relationships with open public providers are the highest risk interactions. It is likely preferable to use a credential provided by a trusted broker or intermediary to protect the integrity of government credentials and systems. A government system using a credential from a trusted intermediary may require a higher level of identity proofing than is present in some of today's common federated credentials such as Facebook, mail provider or OpenID accounts.

Proper understanding of the relationships, level of trust and responsibilities of each of the parties in a cloud based system can be supported in a secure way through intelligent use of identities, persona and credentials.

5 FEDRAMP SECURITY CONTROLS

In November 2010, the FedRAMP program office released a draft set of security controls based on NIST SP 800-53 Revision 3 for both LOW and MODERATE systems. The controls included the specification of control parameters and additional requirements and guidance for the baseline security controls. The controls issued by the FedRAMP program also specified supplemental control enhancements to meet security requirements deemed appropriate by the FedRAMP program office and its Joint Authorization Board. These controls formed the basis of the analysis presented in Section 6 of this paper.

You may obtain the FedRAMP security controls and related guidance from <http://www.cio.gov/pages-nonnews.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP>

6 FEDRAMP-BASED ANALYSIS; SECURITY CONSIDERATIONS

The analysis in this section is aligned to the NIST SP 800-53 baseline security controls for a Moderate impact system with anticipated control baseline adjustments to support the FedRAMP program. Although the NIST guide is final, the FedRAMP supplemental controls are based on a draft which is currently undergoing government review. The reader is cautioned that the final FedRAMP supplemental security requirements/controls will most likely vary from the draft used for this analysis. Therefore, readers should examine the final FedRAMP guidance to identify changes. Additionally, the scope of the analysis was not for all the applicable controls, but rather control implementations deemed unique from typical hosted environments. Finally, the control ownership and implementation solutions presented are examples. The design of the SaaS Email solution and the technologies involved dramatically influence control implementation. The purpose of this paper is to present examples to aid consumers and implementers in understanding how to determine control ownership and some best practices for implementing the requirements/controls.

Cloud Computing Security Considerations and Best Practices for SaaS Email

6.1 G2CM Assumption: Government Access to Certified Provider (Hybrid)

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
Access Control	Provide access control policies to provider. Determines authorized users and communicates changes	Information flow	Implement consumer AC policies Implement access control / account changes specified by consumer Session limits	
Audit and Accountability	Record # of Bytes Sent / Transaction Scheduled review of audit logs as part of standard operations.	Agreed methodology for Correlation of # of Bytes Sent and Bytes received for validation. Agreement to offline storage of audit records.	Provider should examine audit and event logging requirements to select security incident and event management (SIEM) solutions that support the requirements and can scale to provider anticipated consumers. Some consumers may require segregation / no co-mingling of audit/event data with other consumers. Record # of Bytes Received / Transaction Selection of Validated NTP Service for Timestamping of logs and other activities Retain Audit records for at least 90 days online.	The list of auditable events must be jointly agreed and signed off by provider and customer. The minimum required by FedRAMP are: successful and unsuccessful account logon events; Account management events; object access; policy change; privilege functions; process tracking; and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. Both provider and consumer must have the ability to detect and respond to security incidents and events. This response should be coordinated between provider and consumer.
Security Assessment and Authorization	Periodic (at least, annually) risk and security assessment of policies, procedures, and control(s)	Be able to clearly define the boundary/perimeter devices and controls and comply with the federal InfoSec/change controls policies, procedures and requirements to certify and obtain "Authorization to Operate and/or Connect"	Perform periodic security assessments, audits and authorization as required and generate/provide/retain audit records and reports (i.e., artifacts) in compliance with consumer's regulatory requirements and FedRAMP cert. requirement.	G2CM: Government Access to Certified Provider represents "authenticated access via government controlled device" therefore, certain security requirements/controls (e.g., FDCC, FISMA, etc.) should apply to

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
				consumer sites and consumer perimeter devices whereas provider site and its boundary should be protected and certified in compliance with FedRAMP and/or “agreed-upon” governance program(s).
Identification and Authentication	Participate in federated identity Provide credentials to government users. Authenticate user to government network.		Authenticate user via federated identity	
Incident Response	Provide main contact for IR.	Agree to format for delivery of forensic information between provider and Consumer.	Naming and communicating IR personnel.	Provide main contact for IR.
Maintenance	<p>MA-1 Provide system maintenance policy and procedures, and role/responsibility definition to provider. Review and update annually or as change review boards require.</p> <p>Communicate organizational risk strategy to provider.</p> <p>Communicate security information level of content within the environment to provider (for risk level establishment).</p> <p>Review and approve any maintenance-related policies and procedures.</p>	<p>MA –Ensure remote maintenance is performed on an administration network (separate from production).</p> <p>The (WAN-based) administrative network should be maintained with uniform access management and other controls to ensure maintenance activity integrity and auditability across the various cloud nodes.</p> <p>Any external provider access (outside</p>	<p>MA-1 Implement system maintenance policies in a coordinated and consistent manner across the various cloud devices/locations. Confirm roles and responsibilities annually with Agency customer(s) or as respective change review boards require.</p> <p>MA-2 - Validate, perform, control, supervise, and record maintenance on devices across the various cloud nodes (locations) that comprise the hosted email environments.</p> <p>MA-3 – Supervise maintenance activities (tools used, etc.) within all of the cloud nodes to ensure environment integrity. Uniform tools should be used by maintenance vendors.</p> <p>MA-4 and MA-5 - Maintain local or non-local maintenance records across the various cloud locations to provide a</p>	<p>MA-1 – Cloud providers should consider/account for Agency customers’ exiting HW/SW maintenance agreements and how they might be leveraged within the overall maintenance program.</p> <p>MA-3, MA-4 It is advised that maintenance activities be performed uniformly across the various cloud locations/nodes (delivered by the same organizations – ideally with the same personnel servicing the respective locations. - e.g. EMC has a maintenance support agreement with cloud vendor, and designated and pre-approved - U.S. citizen personnel are the ones performing the maintenance activities at the respective cloud locations.) This will greatly facilitate maintenance record-</p>

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
		Agency or provider) to perform maintenance should be issued temporary privileges, with activities supervised, reported and audited by the cloud provider.	<p>customer-relevant, auditable and accountable record of who performed what maintenance activity when.</p> <p>MA-4 -For remote maintenance (or automated activities) – assumed to be common in cloud-based environments, maintain rigorous policies regarding strong authentication and access</p> <p>MA-5 Maintain authorized personnel/vendor list across the various cloud locations (including US citizenship or other controls re: Controlled Unclassified Information (CUI)).</p> <p>MA-6 (FedRAMP) The service provider defines a list of security-critical information system components and/or key information technology components. The list of components is approved and accepted by the JAB</p> <p>MA-6 – (FedRAMP) - Requirement: The service provider defines a time period to obtain maintenance and spare parts in accordance with the contingency plan for the information system and business impact analysis. The time period is approved and accepted by the JAB.</p>	keeping and auditability.
Media Protection	<p>Develop Media Protection Policies and Procedures and provide it to the provider</p> <p>Identify different types of Media, its storage and transport requirements permissible in the</p>		<p>Implement Media Protection policies and procedures</p> <p>Comply with the permissible media storage and transport requirements</p> <p>Achieve JAB approvals for security</p>	

Cloud Computing Security Considerations and Best Practices for SaaS Email

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
	<p>providers environment</p> <p>Adhere to government controlled device policies and procedures related to utilizing and plugging in various media types</p>		<p>measures, personnel's, etc.</p> <p>Document and get the approval of media types utilized within the facility</p> <p>Implement FIPS 140 encryption</p> <p>Segregate media usage between govt and non-govt customers</p> <p>Review and log non compliance and sign-off Media Sanitization</p>	
Planning	<p>Develop, periodically update, and maintain formal security planning policies, procedures, and system security plans for Cloud Computing Service, in accordance with consumer's enterprise risk strategies and security assessment results.</p>	<p>Support and Ensure the devices/controls operate/support security policies, procedures, and requirements in the plan.</p>	<p>Be able to review and assist consumer's security planning activities and support proposed/agreed security requirements and controls, as described in its security plans and action items.</p>	<p>FedRAMP (PL) section appears still in development. (i.e., only 2 generic controls, listed with a few requirements/details.</p>
Risk Assessment	<p>Develop/update/maintain risk assessment policy and procedures, aligned with FedRAMP requirements and guidelines for cloud computing service</p> <p>Perform a periodic risk assessment in compliance with the risk assessment policy and procedures (i.e., every 3 years or when a significant change occurs)</p> <p>Based on risk tolerance level, vulnerability, and information asset categorization as defined and mandated by consumer's risk</p>	<p>Ensure consumer/provider boundaries are clearly defined and reviewed/vulnerability scanned as part of the periodic risk assessment and requirements established by Consumer and Provider.</p>	<p>Develop/update/maintain risk assessment policy and procedures for cloud computing service in coordination with the requirements (e.g., FedRAMP) recommended and/or mandated by consumer (i.e., government agency).</p> <p>Perform a periodic risk assessment and vulnerability scanning/testing, and assist/ jointly review the results with consumer to develop action plans and remediate control gaps and weaknesses.</p> <p>(Note: Remediation requirement would vary based on the consumer's policy and procedures. e.g., high risk</p>	<p>The outcome/results should be used to further develop/update other control domains and areas.</p> <p>(e.g., security planning, operational security assessment/authorization, configuration management, etc.)</p> <p>A significant change is defined in NIST 800-37 Rev. 1 Appendix (F) for the risk assessment.</p>

Cloud Computing Security Considerations and Best Practices for SaaS Email

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
	assessment policy and procedures, periodically perform a vulnerability scanning and produce/review the results.		vulnerability needs to be mitigated within 30 days, medium-risk within 90days, etc.)	
System and Services Acquisition	<p>Develop/periodically update and maintain systems and services acquisition policies and procedures, aligned with FedRAMP requirements and guidelines for cloud computing services and products. (Note: the use of Common Criteria, ISO/IEC 15408) evaluated products are strongly preferred.)</p> <p>JAB - Joint Authorization Board reviews the documents/ assessment results provided by Service Provider and validate, approve/accept security controls, risks, and services from the outsourced cloud services and products.</p>	Ensure perimeter/boundary devices and controls are covered by the control requirements mandated by the corresponding policies, procedures, and acquisition plan(s)/evaluation criteria.	<p>The service provider documents all outsourced security services (e.g., cloud computing) and conducts a risk assessment of future outsourced security services. Also, planned outsource activities need to obtain a formal approval/authorization from the JAB.</p> <p>The provider defines/develops a list/plan of measures to protect outsourced services (i.e., cloud computing) threats and submit the list/plan for JAB's review and approval.</p>	The section appears still under development.
System and Communications Protection	<p>SC-1 (and various subsections of SC) Provide system and communications protection policy (traffic flow, authorized source and destination, denial of service, data in motion, information system partitioning, cryptographic device support, PKI, etc.)</p> <p>Receive communication escalations and updates – and where required make decisions regarding how the cloud environment is to be delivered and controlled (proactively and</p>	<p>Validate authorized source and destination. Agency and provider monitor and control respective communications at the external boundary of the system and at key internal boundaries within the system (For Agencies, this would be the TIC gateway(s) to the cloud email provider(s).) Session authenticity via session identifiers or similar.</p> <p>SC-7(1) (FedRAMP) Requirement: The service provider and service consumer ensure that federal information (other than unrestricted information) being transmitted from</p>	<p>SC-1 (and various subsections of SC) Implement system and communications protection via system architecture and configuration to meet Agency policy/mandates (traffic flow, authorized source and destination, denial of service, data in motion, information system partitioning, cryptographic device support, PKI, etc.)</p> <p>SC-4 – Information in shared resources – Design/maintain solution architecture and operational support model to prevent unauthorized exfiltration of information.</p>	

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
	<p>reactively).</p> <p>Configure end-user devices such that split-tunneling and similar unintended communication paths are prevented.</p>	<p>federal government entities to external entities using information systems providing cloud services is inspected by TIC processes.</p> <p>SC-7(3) (FedRAMP) - Requirements: The service provider defines the internal communications traffic to be routed by the information system through authenticated proxy servers and the external networks that are the prospective destination of such traffic routing. The internal communications traffic and external networks are approved and accepted by JAB.</p> <p>SC-7(2) – additional req (8) – FedRAMP - at least annually</p> <p>SC-5 (FedRAMP) - Requirement: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.</p> <p>Other moderate control requirements SC-7 (8) SC-7 (12) SC-7 (13) SC-7 (18)</p>	<p>SC-32- Compartmentalize the administrative access/functions from the user access/functions (network interfaces, etc.) such that separation is maintained within and across all of the cloud nodes that would comprise this application environment</p> <p>Establish controls such that information from a prior user/administrator is not accessible to a subsequent user/administrator via the shared cloud infrastructure</p> <p>Prevent Denial of Service attacks within the cloud delivery architecture, ideally with expansion and contraction across the cloud sites that are transparent to the users.</p> <p>Maintain primary and secondary DNS services.</p> <p>SC-5 (FedRAMP) - Requirement: The service provider defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list. The list of denial of service attack types is approved and accepted by JAB.</p>	

Cloud Computing Security Considerations and Best Practices for SaaS Email

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
		<p>SC-9 (FedRAMP) - Requirement: The service provider must implement a hardened or alarmed carrier Protective Distribution System (PDS) when transmission confidentiality cannot be achieved through cryptographic mechanisms.</p> <p>SC-10 (FedRAMP) - Parameter: [thirty minutes for all RAS-based sessions; thirty to sixty minutes for non-interactive users] Guidance: Long running batch jobs and other operations are not subject to this time limit.</p> <p>SC-11 (FedRAMP) - [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication] Requirement: The service provider defines the security functions that require a trusted path, including but not limited to system authentication, re-authentication, and provisioning or de-provisioning of services (i.e. allocating additional bandwidth to a cloud user). The list of security functions requiring a trusted path is approved and accepted by JAB.</p> <p>SC-12 (FedRAMP) must be NIST approved</p> <p>SC-15 (FedRAMP) - Requirement: The information system provides disablement (instead of physical disconnect) of collaborative</p>		

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
	<p>SC-28 – The NIST control was designed to protect information at rest with non-mobile devices. With respect to this use case, the situation arises where email data could be accessed and stored on the mobile device as well as the non-mobile IT infrastructure. Measures should be taken by the</p>	<p>computing devices in a manner that supports ease of use.</p> <p>SC-17 (FedRAMP) - Requirement: The service provider defines the public key infrastructure certificate policy. The certificate policy is approved and accepted by the JAB.</p> <p>SC-18 – (FedRAMP) - Requirement: The service provider defines the software applications where the automatic execution of mobile code is prevented by the information system providing cloud services.</p> <p>Requirement: The service provider defines the actions to be taken prior to the information system executing mobile code in the software applications identified. Software applications and actions taken by the service provider are approved by JAB.</p> <p>SC-27 (FedRAMP) - Requirement: The service provider and service consumer define which applications must run independent of operating system. The OS Independent applications list is approved and accepted by JAB.</p> <p>SC-28 and SC-28 (1) (FedRAMP) – Requirement: The service provider and service consumer define what levels of data-level control would satisfy the requirements of the environment. The range of</p>	<p>SC-28 (FedRAMP) - Requirement: The service provider provides encryption solutions at the data level, and has capabilities that can demonstrate where data resides (or has resided) within the environment at any given point in time. This includes primary data storage as well as secondary (backup) storage and other storage</p>	

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
	<p>agency (and user) such that data that is stored on the mobile device is also protected (encrypted) and that policies/technologies are in place to accommodate international travelers (where data may leave the U.S. defined/protected boundary.)</p>	<p>considerations could include data encryption, data sovereignty control (to ensure that resides within allowable domains), and mechanisms to ensure integrity of data at rest. Mechanisms would need to be reportable approved and accepted by the JAB. Another aspect is ensuring that the NIST description of “non-mobile” remains intact with respect to the cloud computing provider given the fluid nature of how data can be moved throughout the cloud computing environment.</p> <p>SC-30 (FedRAMP) - Requirement: The service provider and service consumer define what levels of virtualization visibility are required (if any). These considerations may involve recording which instances are established, moved, changed and decommissioned (and why these administrative changes were made – either per agency direction or provider-justified reasons)</p> <p>SC-32 (FedRAMP) - Requirement – The service provider and service consumer should be in sync regarding the level of compartmentalization in the cloud environment (physical vs. virtual) and that the boundaries are maintained as the environment expands or contracts to satisfy surge demands on the system.</p>	<p>tiers (archival) as required.</p> <p>Additionally, related solution accountability with respect to cloud administrator access to any data (identity management and access control) need to be demonstrable and accountable per agency requirements.</p> <p>All of the above needs to be reviewable, approved and accepted by JAB.</p> <p>SC-28 (FedRAMP) - The service provider internally maintains a virtualization instance record within the environment for technical, billability, and other reasons that may be required by or benefit the agency. One example is forensic analysis that may be required after a security incident where the record of where instances existed would need to be examined.</p> <p>SC-32 – The service provider should institute, maintain and document the compartmentalization throughout its system – to include separations at the network, system data and application levels of the environment. These separations should map to such operational aspects as administrator access, automated operational tasks and incident management analysis.</p> <p>SC-32 – The service provider should</p>	

Cloud Computing Security Considerations and Best Practices for SaaS Email

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
		SC-33 (FedRAMP) – Requirement – The service provider and service consumer should be in sync regarding the integrity of the environment and the data that comprises it. Specifically, no unauthorized or unintended access is allowed within the operational support system structure that may result in the unauthorized deletion or modification of data. This includes the unauthorized access at various information aggregation or protocol transformation points via the network, or intra-system within the cloud provider’s infrastructure.	institute, maintain and document controls to avoid unauthorized access to the environment at any point within the network, system or storage solution tiers that could result in an ability to modify, delete or otherwise manipulate data within the system. This includes user, administrator, or even automated system access. Additionally, the controls should address steady and dynamic cloud computing environment states. Access audits should be performed regularly with appropriate actions performed and communicated to determine root cause and remedy any anomalies or exceptions.	
Program Management	Provide FISMA/other regulatory/compliance reporting requirements to Provider for its continuous monitoring and security program management for cloud services.		Develop a strategy and implement a program for the continuous monitoring of security control effectiveness (including change/supplement the control set in response to any proposed, actual changes to the information systems and/or operating environment)	Provide FISMA/other regulatory/compliance reporting requirements to Provider for its continuous monitoring and security program management for cloud services.

6.2 C2CM: Controlled Access to Certified Provider (Hybrid)

In this access/facility pair, an authenticated User/Device consumes a service provided by a certified provider in a hybrid cloud model

Provider: Commercial Provider whose data center facility has been certified as compliant to a FISMA Moderate level.

Consumer: The service is accessed by authenticated and authorized users. The controlled access users are assumed to access the service from non-government issued desktops, PDA’s and mobile laptops.

Cloud Computing Security Considerations and Best Practices for SaaS Email

Information Categories: The service will contain both restricted and unrestricted data. The service will store documents or data of various types. Some data will meet the criteria for records and are subject to retention schedules. Some data may be subject to legal discovery and hold actions

Assumptions: Some users in the user base will use the public cloud, some a private internal service and some may use both (hybrid).

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
Security Assessment and Authorization	Same as G2CM, with more restrictive security control requirements on the device provision process and configuration managed and owned by non-government entity	Security controls and requirements for Consumer Boundary/ Perimeter Devices, connecting Non-government owned device to the cloud services, need to be assessed/examined carefully before obtaining Authorization to Operate/Connect.		The only difference between G2CM and C2CM models is that the device ownership and origination of the data request/incoming data (i.e., connection points) to the cloud service.
Maintenance	<p>All of the considerations per the 5.3 G2CM: Government Access to Certified Provider (Mixed) Scenario PLUS...</p> <p>Identification/inventory of the non-government issued desktops, PDAs and mobile laptops – in terms of device IDs/types, (home) access locations, and other identifying criteria. Communicate this info to provider per maintenance and support considerations.</p> <p>Consideration of SLAs and functionality/performance assurances to a defined set of end-user/mobile devices. (Not all end user devices would be supported, or uniformly functional per service releases, etc.)</p>	<p>All of the considerations per the 5.3 G2CM: Government Access to Certified Provider (Mixed) Scenario PLUS...</p> <p>Network paths and controls to ensure that non-government issued devices will still need to access the hosted environment via the TIC. (Minimizes network variations and ensures more efficient maintenance activities.)</p>	<p>All of the considerations per the 5.3 G2CM: Government Access to Certified Provider (Mixed) Scenario PLUS...</p> <p>Consideration of both government issued and non-government issued devices when performing maintenance, diagnosis, etc. on the hosted environment.</p>	<p>All of the considerations per the 5.3 G2CM: Government Access to Certified Provider (Mixed) Scenario PLUS...</p>

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
	Issue policy/support guidance to users pertaining to access – particularly pertaining to restricted data. (And that Agency cannot guarantee functionality for any non-government issues/approved devices.)			
Media Protection	<p>Develop Media Protection Policies and Procedures and provide it to the provider</p> <p>Identify different types of Media, its storage and transport requirements permissible in the providers environment</p> <p>Develop the list of media types users/device can utilize form Non-Controlled government devices and restrict the utilization of non verified media types</p> <p>Train users in Media sanitization processes and procedures</p>	Limited or no information flow between user/device with unverified media types attached	<p>Implement Media Protection policies and procedures</p> <p>Comply with the permissible media storage and transport requirements</p> <p>Achieve JAB approvals for security measures, personnel’s, etc.</p> <p>Document and get the approval of media types utilized within the facility</p> <p>Implement FIPS 140 encryption</p> <p>Segregate media usage between govt and non-govt customers</p> <p>Review and log non compliance and sign-off Media Sanitization</p>	<p>Develop Media Protection Policies and Procedures and provide it to the provider</p> <p>Identify different types of Media, its storage and transport requirements permissible in the providers environment</p> <p>Develop the list of media types users/device can utilize form Non-Controlled government devices and restrict the utilization of non verified media types</p> <p>Train users in Media sanitization processes and procedures</p>
System and Communications Protection	<p>All of the considerations per the 5.3 G2CM: Government Access to Certified Provider (Mixed) Scenario PLUS...</p> <p>Identification/inventory of the non-government issued</p>	<p>All of the considerations per the 5.3 G2CM: Government Access to Certified Provider (Mixed) Scenario PLUS...</p> <p>Network paths and controls to ensure that non-government issued</p>	<p>All of the considerations per the 5.3 G2CM: Government Access to Certified Provider (Mixed) Scenario PLUS...</p> <p>In the event of device theft, compromise, etc. – per Agency</p>	<p>All of the considerations per the 5.3 G2CM: Government Access to Certified Provider (Mixed) Scenario PLUS...</p>

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

Control Family	Location/Situation			
	Consumer Site	Boundary	Provider Site	Assumptions/Comments
	desktops, PDAs and mobile laptops – in terms of device IDs/types, (home) access locations, and other identifying criteria. Issue policy guidance to users pertaining to access – particularly pertaining to restricted data.	devices will still need to access the hosted environment via the TIC. Network/host access restrictions to prevent scenarios such as simultaneous access from multiple devices, international access, and similar (except by exception)	direction – lockout users from accessing the environment (at least from that device)	

Cloud Computing Security Considerations and Best Practices for SaaS Email

7 REFERENCES

- a) M-08-16, Guidance for Trusted Internet Connection Statement of Capability Form (SOC) (PDF), Office of Management and Budget, April 4, 2008
- b) Trusted Internet Connections (TIC) Program Reference Architecture Document, Version 1.0, DHS/Federal Network Security, April 20, 2009
- c) Trusted Internet Connections (TIC) Program Reference Architecture Document, DRAFT Version 2.0, DHS/Federal Network Security, June 30, 2010
- d) Trusted Internet Connections (TIC) Update for the Information Security and Privacy Advisory Board, Department of Homeland Security, Federal Network Security, July 29, 2009
- e) Managed Trusted Internet Protocol Services (MTIPS), GSA
- f) SaaS Email Pre-Solicitation Briefing Trusted Internet Connections Challenges For Cloud Computing Providers, Sean Donelan, TIC National Program Manager, DHS/Federal Network Security, November 1, 2010
- g) Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, Draft Version 0.96, Federal CIO Council, November 2, 2010.
- h) Top Threats to Cloud Computing V1.0, Cloud Security Alliance, March 2010
- i) Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines, SANS, Version 2.3, November 13, 2009.
- j) Cloud Computing Use Cases, Version 4.0, Cloud Computing Use Case Discussion Group, 2 July 2010

Cloud Computing Security Considerations and Best Practices for SaaS Email

8 APPENDIX A: RISKS SPECIFIC TO CLOUD COMPUTING AND RECOMMENDED MITIGATIONS/SOLUTIONS

The following sets of tables provide identified elements that would need to be addressed with respect to email software as a service delivery.

8.1 Trusted Internet Connection (TIC) Considerations

Analysis Assumption: Restrictive data moving solely between US Government entities and (FedRAMP) certified providers (G2CM). In addition to the TIC Capabilities listed within Appendix B of *the Trusted Internet Connections (TIC) Program Reference Architecture Document Version 2.0 (DRAFT) Prepared by: Federal Network Security US Department of Homeland Security June 30, 2010*, other considerations are outlined below:

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
8.1.1	Unauthorized or unintended access to the environment through the TIC	Loss of environment availability/functionality	Internal agency employee or employee of service provider/contractor intentionally or unintentionally accesses the system and makes modifications rendering the system inoperable	S.2, S.3
8.1.2		Unauthorized disclosure or access to information	Internal employee or employee of service provider/contractor intentionally or unintentionally accesses and/or captures data from the environment	S.2, S.3
8.1.3		Compromise of auditability / accountability	Geographically-distributed cloud architecture obscures administrator/user auditability	S.2, S.3, S.9
8.1.4		Loss of system or data integrity	Internal agency employee or employee of service provider/contractor intentionally or unintentionally accesses the system causing degradation in the accuracy, quality or consistency of the data/system environment	S.2, S.3
8.1.5	Lack of sustained TIC compliance within and across cloud delivery nodes	Compliance complexity	TIC compliance requirements were not determined with cloud architectures in mind. Risks exist for cloud computing providers to be compliant with TIC controls – particularly if they vary between/across Agencies.	S.4, S.5
8.1.6			Challenging or protracted process for auditors to determine compliance of cloud computing environments with respect to TIC compliance requirements. Getting Authority to Connect (ATC)	S.5

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
			could be challenging.	
8.1.7			Different vendor cloud computing solution architectures may create conflict where uniform TIC configurations are difficult to achieve or maintain within/across the Agencies or TICAPs	S.6, S.8
8.1.8		Compliance compromise	Changing/fluid nature of cloud delivery complicates or obscures auditable processes and procedures required to maintain TIC compliance (A&A).	S.12, S.13
8.1.9			Data could be delivered from locations that are not approved TIC locations (which may fall out of compliance depending on the cloud network delivery architecture).	S.4
8.1.10			Controlled/ directed access thru TIC nodes creates concentrated risk (per end user access, system integrity, etc.) in the event that these nodes were compromised.	S.4, S.5, S.11
8.1.11	Cross Domain Risks	Lack of accessibility or security controls across network domains	Information accessible by one domain may not be accessible by another domain due to the security rules – and this would likely be controlled at the network layer, presumably an element within the TIC. Cross domain limitations may restrict access to the email environment for certain users. Or (perhaps worse), users may unknowingly send or receive data meant for one defined security domain level, but instead traverses another.	S.4, S.11
8.1.12	Technical issues or incompatibility	Loss of system functionality or performance degradation	Changes are required or made within an Agency’s TIC configuration – or within a cloud vendor’s computing environment - that impact the functionality of the cloud computing environment (port restrictions, etc.)	S.10, S.12, S.31
8.1.13			Fluid, cloud-like delivery changes are made within a vendor’s cloud computing environment – (e.g. to serve surge demand) that may not be compatible with TIC configurations.	S.6, S.9, S13,
8.1.14			Geographic and/or network “hop” distance between TIC gateways and cloud computing provider hand-off points may be less than optimal (particularly for large email files or other heavy-load transactions)	S.7, S.8

Cloud Computing Security Considerations and Best Practices for SaaS Email

8.2 Boundary Constraints and Multi-Tenancy

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
8.2.1	Internal - Intentional	Data Exfiltration	Internal employee or employee of service provider/contractor intentionally making data available across intended boundaries.	S.17, s.17a
8.2.2	Internal - Accidental	Data Exfiltration	System failure inadvertently allows data to be visible across intended boundaries.	S.17
8.2.3	External - Neighbor	Data Exfiltration	A neighbor intentionally attacks a weakness to facilitate data infiltration on a neighbor	S.17, S.17a
8.2.4	External - Non-neighbor	Data Exfiltration	A fully external threat attacks a weakness to facilitate data infiltration beyond the system boundaries.	S.17, S.17a
8.2.5	External	Confidentiality Compromise Unauthorized disclosure or access to information	Client Device: Loss of device and cached or stored information	S.18
8.2.6	External	Confidentiality Compromise Unauthorized disclosure or access to information	Client Device: Transfer of information to a domain without proper access controls (cut/paste, shared area on device)	S.21, S.22
8.2.7	External	Confidentiality Compromise Unauthorized disclosure or access to information	Client Device: Shared Device exposes one user's data to another	S.21, S.22
8.2.8	External	Confidentiality Compromise Unauthorized disclosure or access to information	Network: lack of strong separation between flows	S.19, S.21, S.22

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
8.2.9	External	Confidentiality Compromise Unauthorized disclosure or access to information	Network: uncontrolled device cache access	S.22
8.2.10	External	Confidentiality Compromise Unauthorized disclosure or access to information	Storage: potential for access by unauthorized users (weak access controls)	S.20, S.22
8.2.11	External	Confidentiality Compromise Unauthorized disclosure or access to information	Storage: administrator has broad permissions to access	S.22, S.17a
8.2.12	External	Confidentiality Compromise Unauthorized disclosure or access to information	Storage: data copy ACL not tied to primary copy access control changes	S.22
8.2.13	External	Confidentiality Compromise Unauthorized disclosure or access to information	Storage: ability to read deleted data on shared device	S.22, S.23
8.2.14	External	Confidentiality Compromise Unauthorized disclosure or access to information	Storage: cache or memory separation or residual copy accessible	S.17, S.19, S.22, S.25a
8.2.15	External	Confidentiality Compromise Unauthorized disclosure or access to information	Server: use of "superuser" permissions on server processes can allow unauthorized access	S.22, S.17a, S.23
8.2.16	External	Confidentiality Compromise Unauthorized disclosure or	Server: trusted boot issues	S.25a

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
		access to information		
8.2.17	External	Confidentiality Compromise Unauthorized disclosure or access to information	Server: memory or cache access to live or residual copy	S.17, S.19, S.22, S.25a
8.2.18	External	Confidentiality Compromise Unauthorized disclosure or access to information	Server: virtual servers are files that can be stopped and read	S.17, S.22, S.23
8.2.19	External	Confidentiality Compromise Unauthorized disclosure or access to information	Printer: routing of copies to remote device	S.22, S.17
8.2.20	External	Confidentiality Compromise Unauthorized disclosure or access to information	Printer: cache or imprint (residual copy)	S.17, S.23, S.22
8.2.21	External	Confidentiality Compromise Unauthorized disclosure or access to information	Printer: spooler cache not controlled	S.22
8.2.22	External	Confidentiality Compromise Unauthorized disclosure or access to information	Camera: ability to see information	S.22
8.2.23	External	Confidentiality Compromise Unauthorized disclosure or access to information	Microphone: ability to overhear conversation	S.22

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
8.2.24	External	Confidentiality Compromise Unauthorized disclosure or access to information	Printer: media transformation (uncontrolled paper disposal, theft)	
8.2.25	External	Confidentiality Compromise Unauthorized disclosure or access to information	Facility: legal seizure of shared device	S.22
8.2.26	External	Confidentiality Compromise Unauthorized disclosure or access to information	Facility: unauthorized access to physical device (access to multi-tenant machine room)	S.22
8.2.27	External	Integrity Compromise Unauthorized alteration of information	Client: shared device without adequate separation of information access rights allows unauthorized changes	S.23
8.2.28	External	Integrity Compromise Unauthorized alteration of information	Client: single domain machine access multiple systems or domains	S.25a, S.23, S.17, S.22
8.2.29	External	Integrity Compromise Unauthorized alteration of information	Client: malware allows root access to machine	S.22, S.23, S.24, S.25
8.2.30	External	Integrity Compromise Unauthorized alteration of information	Client: cross domain attacks	S.17, S.17a, S.25
8.2.31	External	Integrity Compromise Unauthorized alteration of	Network: transaction intercepted, changed, deleted or replaced to affect data integrity	S.24, S.25, S.22

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
		information		
8.2.32	External	Integrity Compromise Unauthorized alteration of information	Network: shared cache on CDN, acceleration devices allows change access	S.24, S.25, S.17
8.2.33	External	Integrity Compromise Unauthorized alteration of information	Storage: shared storage device allows access to modify or affect data integrity	S.24, S.25, S.20-22
8.2.34	External	Integrity Compromise Unauthorized alteration of information	Server: SQL injection or other attacks allow access to modify data on shared server	S.25, S.25a, S.21, S.22
8.2.35	External	Integrity Compromise Unauthorized alteration of information	Printer: ability to change or falsify printed output once printed	S.25b
8.2.36	External	Integrity Compromise Unauthorized alteration of information	Facility: physical attack against domain controller or other server	S.17a, S.19, S.21, S.23
8.2.37	External	Availability Compromise Unauthorized destruction or loss of access to data	Client: single tenant consumes all available resources	S.25c, S.17a, S.23
8.2.38	External	Availability Compromise Unauthorized destruction or loss of access to data	Client: accidental or intentional destruction or deletion of data	S.21, S.17a, S.25

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
8.2.39	External	Availability Compromise Unauthorized destruction or loss of access to data	Network: bandwidth congestion restricts access to data	S.25c, S.17a, S.23
8.2.40	External	Availability Compromise Unauthorized destruction or loss of access to data	Network: proxy or caching of data faults and loses some transactions	S.24, S.25
8.2.41	External	Availability Compromise Unauthorized destruction or loss of access to data	Storage: legal hold or device seizure denies other tenants access to data	S.25
8.2.42	External	Availability Compromise Unauthorized destruction or loss of access to data	Storage: one tenant deletes data that is critical to another	S.20, S.21
8.2.43	External	Availability Compromise Unauthorized destruction or loss of access to data	Server: shared server faults and denies multiple tenants access to services	S.25
8.2.44	External	Availability Compromise Unauthorized destruction or loss of access to data	Server: poorly configured failover causes migration thrashing	S.25c
8.2.45	External	Availability Compromise Unauthorized destruction or loss of access to data	Server: resource allocation among tenants leads to slowdown in processing (load balancing)	S.25c
8.2.46	External	Availability Compromise Unauthorized destruction or loss	Printer: large demand from one tenant delays access to printed output	S.25c

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
		of access to data		
8.2.47	External	Availability Compromise Unauthorized destruction or loss of access to data	Print/fax: purge of queue causes loss of output	S.21
8.2.48	External	Availability Compromise Unauthorized destruction or loss of access to data	Fax: congestion among multiple tenant delays or prevent incoming or outgoing data in a timely manner	
8.2.49	External	Availability Compromise Unauthorized destruction or loss of access to data	Facility: outage impacts multiple tenants	

8.3 Identity Management and Access Control

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.7)
8.3.1	ACCESS IS LOST /DENIED /FEDERATED MODEL	DENIAL OF SERVICE	DENIAL OF SERVICE	S.12
8.3.2	ACCESS IS SUBVERTED /REDIRECTED /FEDERATED MODEL	DISCLOSURE/IDENTITY SPOOFING	EMAIL SPOOFING/IDENTITY THEFT	S.13
8.3.3	Undisclosed financial distress or change of	Controls degrade	All	S.14

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.7)
	ownership			
8.3.4	Domain bleed over	Multi-tenancy Domain bleedover	Loss of confidentiality	S.15
8.3.5	Insider threat	Inappropriate use of admin	Loss of confidentiality	S.16

8.4 Data Security, Ownership and Retention

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
8.4.1	Accidental or unlawful destruction or loss of Data (Availability Threat)	Reliability and Trust - Lack of data center reliability (misconfigurations, lack of updates, patch management, etc.)	Loss of physical control of the data	S2, S4,S19,S22, S36
8.4.2		Storage Error - Cloud distributed architecture (back-up) and design limitations. (multi server back-up of data across geographic locations may not support dynamic updates to data depending on the cloud architecture adopted by the provider)	Non-Compliance of federal mandates for data retention and security	S5,S6,S9,S14, S34,S37,S41
8.4.3		Business Process - Bad business practices. For example, not destroying/erasing data and information during the decommissioning process of the cloud storage or partially deleting or archiving of data by the provider	Loss of intellectual property	S10,S31,S33

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
8.4.4		Cross Platform/Diversity of Platforms Discrepancies - Lack of technology standards across different cloud platforms may result in data loss in translation or transmission.		S5
8.4.5		Data Fragmentation - If data is fragmented and stored in a distributed architecture. Loss of one or many data stores may result in partial data loss and data integrity issues.		S11
8.4.6	Unauthorized alteration of Data (Integrity Threat)	Absence of control over data encryption keys and algorithms	Misrepresentation of data	S11,S23,S24,S19
8.4.7		Absence of access controls	Business process transactional integrity compromised	S34,S19
8.4.8		Business Process - Absence of information governance, risk and compliance controls		S33
8.4.9		Absence of standards to update, retrieve, modify, and update data in cloud. For e.g. Adopting of Cloud Data Management Interface (CDMI) could help.		S35
8.4.10		Absence of control over defining physical, logical, and personnel access controls. At the mercy of the Cloud provider and its processes.		S34
8.4.11		Unauthorized disclosure or access of Data	Absence or limited availability of security policies and structure from the cloud provider that may or may not reflect the security	Jurisdictional limitations. Unauthorized entities (nations) may be able to subpoena data for

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
	(Confidentiality Threat)	posture of consumer.	disclosure otherwise considered confidential.	
8.4.12		Lack of management and operations controls and oversight defining data handling, retention, and disposal.	Data available to administrators/personnel of the cloud providers. E.g. Google Site Reliability Engineer listening Google Voice and reading emails	S33,S38,S36
8.4.13		Lack of data exchange standards for Cloud interoperability resulting in disclosure of data	Failure to meet regulatory and legal requirements.	S9,S11
8.4.14		Non classification of data for data security		S19

8.5 Incident Response and Forensics

This section includes discussion on added complexities which arise from the new actors introduced into the IR and Forensic process when in a multi-tenant cloud. Previously, while an organization might have to deal with multiple departments in an IR scenario, all of them were under the same senior management. In a Cloud scenario, since the Actors are from different organizations, they are likely to have very different charters on Risk tolerance and situational transparency. These differences, if not identified and reconciled before the instantiation of the cloud could result in direct conflict between the cloud customers.

A second issue which arises in the Cloud, which is not new but worthy of mention, is remote forensic activities. Where-as in the past Forensic Analysts may not have had physical access to the systems they were working with, in a Cloud environment, those analysts would definitively not have physical access. The analysts from organizations which embrace the cloud must be prepared with the appropriate tools and processes to handle remote operations.

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
8.5.1	Coordinating personnel in different	The time the Threats remain unresolved could be extended due to lack of	<ul style="list-style-type: none"> Compromises could occur while the Threat is known, but not resolved. 	S.39

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
	organizations when there is a identified threat	cooperation.	<ul style="list-style-type: none"> Compromised systems in a cloud could be used to springboard to others. 	
8.5.2	Coordinating personnel in different organizations during Incident Response	The time to react to an Incident could be increased.	Data or credentials could be leaked during the extended response.	S.40
8.5.3	Coordinating with different organizations during forensic investigation	Time to complete an investigation could be extended or indefinitely put on hold without cooperation from all cloud customers.	Inability to confirm an incident or understand true extent of incident.	S.40
8.5.4	There is no single group to set priority during an incident response	Since each organization will have their own priorities, in an attack which affects multiple customers in a cloud there will be difficulty in deciding how to prioritize resources.	Further compromises or data leakage could occur due to delays.	S.40
8.5.5	The owners of each system need to have compatible tools for forensic analysis	Often different organizations use different proprietary tools for the capture of forensic data. If there isn't standardization between the organizations, the ability to coordinate is curtailed.	Inability to easily trade new rules, settings and pcaps could slow response to issues.	S.39
8.5.6	Other users of the same hosting site may not apply the same level of security controls	Infection vector may come from other sites within the same hosting location	Attack jumping from site to site internally, which is easier from external	S.39
8.5.7	Shutting down or isolating a system in case of an incident may not be possible due to shared resources	Considering that a cloud system can have multiple VMs running on a single piece of hardware, the ability to quarantine the hardware in case of an Incident is not feasible.	Unable to perform standard forensic practices	S.40
8.5.8	Identical defenses between hosted sites allows for distributed attack	If the cloud provider defines a single method of security across all of the sites, then an attacker could do a distributed attack against each of the sites, which	Attackers have a larger attack vector	S.39

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
		might not be cause unless there is correlation between them all. This would allow the attackers more opportunities to breach the security.		
8.5.9	Separate Network session capture & storage of capture for forensics	If the network traffic for each of the sites is stored in a different location there is no way to correlate the traffic in case of an incident	Unable to coordinate analysis	S.26
8.5.10	Separate SIEM managed by each site	If the Log management system for each of the sites is stored in a different location there is no way to correlate the traffic in case of an incident	Unable to coordinate analysis	S.27
8.5.11	All personnel involved in the cloud, including both the cloud proprietors and other customers may be part of the chain of custody of evidence.	For evidence to remain legal it needs to have a documented chain of custody. All involved parties will need to follow the rules to keep a proper chain of custody.	Unable to perform standard forensic practices	S.40
8.5.12	Management infrastructure as an attack vector	If the management of the provider is successfully attacked it could be a vector for all of the hosted systems to become infected.	Unable to perform standard forensic practices	S.39
8.5.13	Multiple customers become infected and each chooses to take a different approach to remediation.	If each organization takes a different approach to remediation it may not result in the issue being resolved.	Attack continue to jump from site to site internally, which is easier from external	S.36
8.5.14	Physical compromise response	In case of a physical incident, there will need to be an agreed upon plan to investigate the physical attack.	Unable to perform standard forensic practices	S.40
8.5.15	If one cloud site is compromised should all others be informed?	If there is an incident in one resident of the cloud, there may be resistance on the part of that resident to communicate to the other residents about the issue. Even	Residents may be under risk but not be informed.	S.33

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
		though it could have a direct impact on those other residents.		
8.5.16	Cryptography and Key Management – Making sure the right keys are available to the investigation team	Cryptographic Keys may be hosted in a Hybrid system. In that case there needs to be a method to ascertain the keys can be available in case of an incident response.	Further compromise while delays occur	S.40
8.5.17	Synchronized and assured time between different cloud customers	If different cloud residents use different time systems it could complicate a response since activities might show up out of order in a coordinated review.	Wrong conclusions or delays introduced by conflicting data	S.39

8.6 Governance, Security Authorization and Continuous Monitoring

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
8.6.1	Security controls and monitoring not implemented on all parts of the cloud solution exposing system/data to numerous threats.	Undefined or unmanageable system or geographic boundaries permit devices/components to be added to the cloud environment to meet consumer demand or new services. These devices / components may not be configured and tested to meet security requirements. NIST SP 800-37	Consumer data located outside of geographically boundary placing data in other countries subject to non-US laws. Risk to unauthorized access to data and system increased.	S.28
8.6.2	Abuse and Nefarious Use of Cloud Computing resources	Consumer registration process does not perform necessary vetting permitting spammers, malicious code authors, and other criminals the ability conduct their	Disruption of service, unauthorized access to data, via Password and key cracking, DDOS, launching dynamic attack points, hosting malicious data,	S.29

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
	CSA Threat #1	activities within the Cloud.	botnet command and control.	
8.6.3	Malicious Insiders via weak access control and personnel practices CSA Threat #3	Provider processes for employee access control to physical and virtual assets combined with hiring standards and practices which provide means for malicious insider to have broad access and limited means of detection.	Unauthorized access to data, Reputation damage, financial impact, productivity losses	S.30
8.6.4	Data isolation between tenants data not maintained during implementation of changes/upgrades CSA Threat #4	Cloud user data segregation not enforced on shared technology permitting personnel from one consumer having access to another consumers data.	Disk partitions, CPU caches, GPUs, and other shared elements may not be designed for strong compartmentalization. This permits attackers to focus on how to impact the operations of other cloud consumers, and how to gain unauthorized access to data.	S.31
8.6.5	Inability to understand risk posture due to rapid pace of change and inability of provider to identify vulnerabilities to the cloud consumer. CSA Threat #7	Cloud provider unable to capture/collect and report critical security risk management metrics and provide in a timely fashion to the consumer. NIST SP 800-37 Continuous Monitoring	Cloud consumer unaware of significant changes in risk poster which increase risk to operations and data.	S.32
8.6.6	Data and Control ownership/responsibility (i.e., custodianship) may not be	Due to undefined/unclear ownership of security incident reporting, control ownership, and other responsibility, Cloud Provider/Consumer may not know a	Increased downtime, delayed escalation/response time, and security incident reporting (CIRT/NIRT) - Continued, wide-spread compromise	S.33

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
	transparent/clearly defined.	proper escalation and reporting channel to submit unauthorized access, change and malicious cyber attacks		
8.6.7	Provider employee access to the customer data and SODs in place are unknown	Cloud Provider doesn't define their employee access to customer's Sensitive, PII, confidential data and no Segregation Of Duties (SOD) is enforced.	Cloud Customer may not know how its PII/Sensitive Data is managed and fail to identify/implement control points that would lead to potential Data Loss, Abuse, and Leakage to other Cloud customers/public domain.	S.34
8.6.8	Lack of security standards/governance/certification program for the cloud computing risk management practice and security requirements	No baseline/security requirements defined/applied/enforced consistently; therefore there is no minimum level of security control/layer considered or implemented. (Security Models and Standards are still emerging)	Security vulnerabilities/issues unique to the Cloud can be easily targeted, exposed, and compromised if there is no mandated/required basic security baseline/SOPs.	S.35
8.6.9	Customer data may be stored in multiple locations; therefore it may not be easily retrievable in a timely manner (e.g., when demanded by authorities)	Data is stored anywhere in the cloud, so it may be difficult to meet/respond/coordinate with the authorities and meet data compliance requirements. In addition, physical location dictates jurisdiction and legal obligation.	Multiple legal requirements/regulations may apply to the customer's data; that makes the customer meet/obtain a full data compliance/unqualified audit opinion very difficult.	S.36
8.6.10	Cloud Provider doesn't understand Customer's compliance/Audit (SAS 70, Trust Service, etc.)	Unlike regular IT service provider/supplier contracting, the cloud provider may not/is not likely to implement the controls specified by the customer.	Due to the lack of understanding and/or failure to negotiate/put the audit requirement in writing, Cloud Provider could mis-configure/fail to implement necessary/required controls.	S.37

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
	requirements and risk profile; or Cloud customer failed to negotiate the control implementation when the provider refused to enforce/directly implement controls required by the customer		Customer/Provider may not be able to pass IT/InfoSec audit(s); hence meet/demonstrate regulatory and compliance requirement(s) and obtain "unqualified" opinion.	
8.6.11	Inability of the cloud provider to clearly identify the system boundary, including assets, IPs, SW, etc.	Cloud Provider does not have a thorough understanding of where the customer data is going to reside and will not be able to implement adequate protection measures across the entire boundary. NIST SP 800-37	Without a clear understanding of what is included in the environment, the Cloud Provider may be unaware of significant weaknesses to the environment that could be exploited by both internal and external threats.	S.38
8.6.12	Lack of a clear definition of security control responsibility between the cloud provider and customer subscribing to the cloud services	Certain controls must be implemented on the user side of the cloud application and without a clear identification of these controls and specific implementation by customers, the entire environment may be vulnerable to an attack. NIST SP 800-53	The data residing in the cloud environment may be exposed to unauthorized access if the customer subscribing to the cloud services does not understand or implement their control responsibilities.	S.39
8.6.13	Data leakage into the cloud environment. Due to the nature of cloud computing, it is nearly	The cloud computing application may be unavailable for an extended period of time if there is an instance of data leakage	Customer operations relying on the cloud application may come to a halt until the forensic analysis is complete.	S.40

Cloud Computing Security Considerations and Best Practices for SaaS Email

ID	Threat	Vulnerability	Risk	Mitigation & Solutions (See Section 8.10)
	impossible to determine the location of where specific data elements reside. If there is a spillage or compromise of the data that requires forensic analysis, the entire environment may need to be taken offline.	requiring forensic analysis.		
8.6.14	Cloud providers may not have a clear understanding of FISMA requirements versus other standards (ISO, HIPPA, SOX, etc.) that they are currently implementing in their environment.	Cloud providers may not understand the complexity and level of detail of the controls identified in NIST SP 800-53 and may not have the capability of implementing some controls without re-engineering of the solution (2 factor auth, warning banners, FIPS 140-2 compliant encryption, etc.).	Cloud providers may not be able to implement specific NIST required controls, potentially compromising the data of the customers using the solution. Additionally, cloud providers may not understand the required time and costs incurred to implement solutions that are compliant with the Federal requirements.	S.41
8.6.15	Implementation of continuous monitoring activities has not been clearly defined.	Cloud providers and customers do not completely understand the continuous monitoring requirements for the Federal government. These requirements are being defined, however, without a clear understanding of this, the providers cannot determine the level of effort or cost of doing business with the Federal government.	If the continuous monitoring requirements are too strict, the cloud providers may not be able to meet the continuous monitoring requirements identified by the Federal government without substantial increases in costs to perform the service or re-engineering of the solution. Alternatively, if the requirements are too weak, the government may not have adequate assurances that their data is being protected.	S.42

Cloud Computing Security Considerations and Best Practices for SaaS Email

8.7 Solutions and Best Practices

The table below presents a collection of best practices and solutions which can be used to address security risks identified in section 8 and mandatory regulatory compliance.

Solution ID	Best Practice / Solution to Mitigate Risks
S.1	Obtain Trusted Internet Connection (TIC) services from a DHS certified provider, e.g., Managed TIC services from a Networx provider.
S.2	Identity and access management controls need to be established and maintained within the TIC, TICAP providers, and cloud computing vendor administrative personnel.
S.3	Ensure backup capabilities are established and maintained – including end user data, administrator access information, network and system log information, and other operational metrics such that rollback or analysis could be supported.
S.3a	Identify, logically separate, and provide TIC PO with data feeds from US Government to external entities
S.4	The vendor must demonstrate an effective capability to enable TIC inspection, and eventual intrusion prevention, of data between government and non-government cotenants/entities.
S.5	Viability and validation of the vendor’s architecture/design are strongly recommended to ensure compliance with TIC requirements.
S.6	Scenario-based run-throughs with email SAAS vendors to understand what would happen under different operational situations would go a long way to elucidate any risks or incompatibilities with TIC-security requirements
S.7	Implement email application constraints with respect to maximum attachment sizes, number of recipients
S.8	Engage industry partners to propose and develop multiple innovative ways to demonstrably meet the requirements
S.9	Establish routine and surprise audits - many can be continuous-monitoring based - to ensure the vendor's compliance with the required standards
S.10	Document the change management process, and have participation from both the email hosting provider and the Agency re: Change Review Boards to ensure that proper communication and respective decision making are achieved.
S.11	Audit the domain tiers to ensure data segregation is maintained. Exercises can be coordinated and planned to ensure that adequate protections and incident response measures are in place.
S.12	Establish audits/reviews of processes and technology used to capture TIC-related information (logs, anomaly/incident reports) on a bi-annual basis. If any TIC-related changes are planned by the external provider or Agency – ensure that they are brought forth before a joint CRB prior to implementation. Craft delivery SLAs to align Agency requirements and vendor commitments.
S.13	Include delivery elements beyond just data capture – and address the delivery integrity of the hosted provider (specifically the network-based TIC elements) as a whole.
S.14	Continuous Monitoring of Financials, human capital
S.15	Air gap, Segregation of networks

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

Cloud Computing Security Considerations and Best Practices for SaaS Email

Solution ID	Best Practice / Solution to Mitigate Risks
S.16	Cleared employees, human capital controls
S.17	Content Scanning (Proxy) - monitor traffic across boundary and flag exceptions (inbound or outbound) based on organizational policy
S.17a	Activity Monitoring (Pattern or Anomaly detection) - monitor activity on systems and between systems for anomalous behavior that might indicate threats against data, users or systems Network monitoring can be done through multiple technologies which involve deep packet capture and inspection. Either via agent based solution for internal communications or network based solutions for between systems.
S.18	PREVENTION: Open Access - all access is allowed, activity is monitored - Emphasis on obligation to share
S.19	PREVENTION: Controlled Access - access is restricted to approved and known users. Emphasis on need to know
S.20	PREVENTION: Physical Separation - each tenant uses a separate physical instance - no reliance on software or configuration to enforce separation
S.21	PREVENTION: Virtual Separation - each tenant gets a separate virtual instance - reliance on virtualization controls, software and configuration to enforce separation
S.22	PREVENTION: Cryptographic Separation - tenants share physical or virtual resources - separation is enforced by encrypting all information in shared resources - reliance on strength of cryptography and use of physical or virtual separation when information must be operated on when not encrypted
S.23	DETECTION: Auditing - tracking all activity against a resource (who, what, when, where) - focus is forensic although could be monitored more real time
S.24	DETECTION: Hashing - generating a value that captures the state of information resources. Can be generated and compared with a stored value to detect change - focus on data integrity
S.25	MITIGATION: Redundancy - making multiple copies of information and storing them at separate locations. Ensures availability if other copies are not accessible and can be used to verify data integrity by comparing for changes
S.25a	TRUST: Use of TPM and other hardware features to ensure trusted separation and policy enforcement
S.25b	INTEGRITY: Support secure printing with physical authentication before printing output
S.25c	AVAILABILITY: Resource limiting/throttling, may be priority based
S.26	Prepared to provide PCAPs
S.27	Prepared to provide logs in CEF format
S.28	Decompose the cloud solution into manageable subsystems (GSS and Applications). Each can have an appropriate FP 199 impact value, security controls and associated boundary inheriting controls where applicable. Augment with "Type" accreditation approach supplemented with robust configuration and change management.
S.29	Stricter initial registration and validation processes. Enhanced credit card fraud monitoring and coordination. Comprehensive introspection of consumer network traffic. Monitoring public

Cloud Computing Security Considerations and Best Practices for SaaS Email

Solution ID	Best Practice / Solution to Mitigate Risks
	blacklists for one's own network blocks.
S.30	Enforce strict supply chain management and conduct a comprehensive supplier assessment. Specify human resource requirements as part of legal contracts. Require transparency into overall information security and management practices, as well as compliance reporting. Determine security breach notification processes.
S.31	Change management and security impact analysis
S.32	Reporting security metrics defined in CyberScope. Disclosure of applicable logs and data. Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls, etc.). Monitoring and alerting on necessary information.
S.33	Governance and ownership issues (i.e., transparency) should be discussed, clearly defined, and assigned as part of the contract/SLA.
S.34	Cloud Customer should request and obtain information related logical access controls in place to enforce proper SOD and also examine its operating effectiveness through C&A/other audit (control testing).
S.35	Develop a Federal standard with recommended best practices, and baseline requirements for the Cloud Computing and Security Issues. e.g., FedRAMP.
S.36	SLAs and Data Ownership/Custodianship needs to be clearly defined and any legal requirements/regulations apply to the customer data on the Cloud should be included in the formal BIA/Risk Assessment.
S.37	Right to Audit clause/SAS 70 Type II/other audit requirement may need to be included in the contract and need to be provided to the customer when required/mandated by authorities/external auditors.
S.38	Clearly define the system boundary and implement strong configuration/change management procedures to ensure that new HW/SW is introduced in a controlled manner.
S.39	Early in the implementation of the cloud service, the Cloud Provider and the customer key stakeholders must determine the responsibility and implement each control prior to releasing customer data into the environment.
S.40	Define clear processes for handling forensic analyses prior to implementing the cloud solution to minimize the impact to operations.
S.41	The government should clearly indicate the security requirements in Requests for Proposals for cloud computing services, indicating the FIPS categorization requirements for the data processed and stored in the cloud solution. Additionally, the government should clearly indicate if a specific FISMA audit using NIST SP 800-53A assessment procedures is required prior to releasing Federal data into the environment, or if the government will accept alternative independent audit opinions already rendered to the cloud provider (SAS 70 Type II, ISO Certification, etc.). Cloud providers should gain an understanding of the FISMA requirements prior to committing to implementation dates in the Federal space because the requirements may be substantially different than what they are currently implementing.
S.42	The government and cloud providers should determine what is feasible from a requirements and operational perspective to meet the intent of the continuous monitoring requirements. Specifically, the cloud providers may be able to provide periodic vulnerability scan results, POAM remediation

Cloud Computing Security Considerations and Best Practices for SaaS Email

Solution ID	Best Practice / Solution to Mitigate Risks
	<p>status, regular intervals of documentation updates, and a summary of changes that have been made to the system. The government may not be involved in all continuous monitoring activities that they would expect from an in-house solution, however they should be able to receive enough information to gain a level of comfort that the activities are being performed. Whatever the solution is determined to be, the requirements should be clearly identified in solicitation documentation (RFPs, RFQs, etc.) so cloud providers can accurately plan for the level of effort.</p>