Contents

This page intentionally left blank

Exhibits

This page intentionally left blank

1 Introduction

1-1 Purpose

The Postal Service™ is committed to creating and maintaining an environment that protects Postal Service information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction. This handbook establishes the information security policies and requirements to protect information resources in a cloud computing environment.

A cloud computing environment must do the following:

a. Protect information resources critical to the Postal Service.

b. Protect information as mandated by federal laws, regulations, directives, law enforcement and judicial processes, and industry requirements.

c. Protect the personal information and privacy of employees and customers.

d. Reinforce the reputation of the Postal Service as an institution deserving of public trust.

e. Meet or exceed Postal Service due diligence standards for the protection of information resources.

f. Assign responsibilities to relevant Postal Service officers, executives, managers, employees, contractors, partners, and vendors.

1-2 Scope

Information security applies to all Postal Service information resources, organizations, and personnel.

1-3 Background

The Privacy Act of 1974, 5 U.S.C. § 552a25, as amended, requires the protection of personal information. The Federal Trade Commission's Fair Information Practices have established a framework under which individuals can depend upon certain privacy-related rights and expectations when engaging in business transactions with both online and brick-and-mortar merchant entities.

The Office of Management and Budget Memorandum M03-22 establishes the guidance for development of Privacy Impact Assessments to enable organizations to understand the privacy implications of the data that they are managing within their systems and to ensure that the proper controls are in place to protect the data according to established law. These provisions have come to be recognized as the basic privacy rights of individuals.

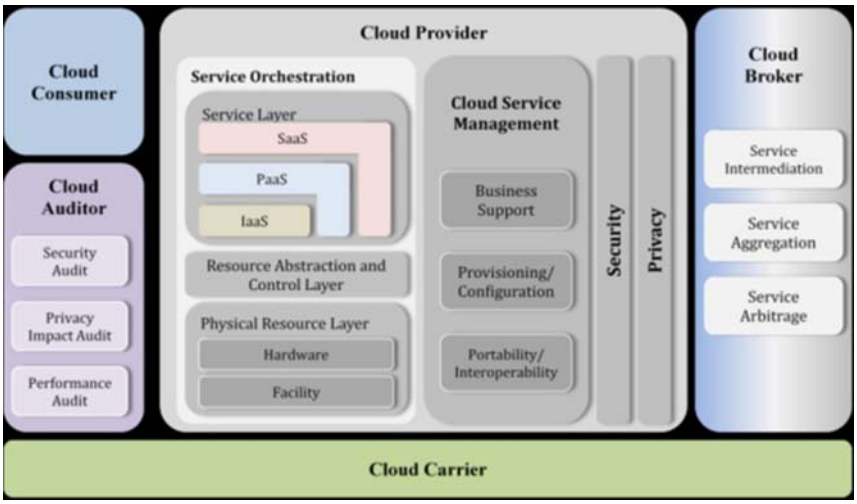
Cloud computing leverages economies of scale, balancing resources among partners that include cloud providers, brokers, and other stakeholders. Cloud computing potentially runs the risk of undoing the trust and confidence that individuals have come to expect of the Postal Service with respect to handling their personal data. Therefore, the Postal Service is challenged to maintain and sustain that confidence level while maintaining a chain-of-trust across the architecture and legal structures established with their cloud providers (CPs).

Exhibit 1-3 presents an overview of a cloud computing architecture, which identifies the major actors, their activities, and their functions in cloud computing. The exhibit depicts a generic high-level architecture and is intended to facilitate the understanding of the requirements, uses, characteristics, and standards of cloud computing.

The high-level cloud computing architecture defines five major actors which are defined below.

Each actor is an entity (i.e., a person or an organization) that participates in a transaction or process and performs tasks in cloud computing.

Exhibit 1-3
Conceptual High-Level Model



The five major actors are defined as follows:

a. **Cloud consumer.** Person or organization that maintains a business relationship with, and uses service from, CPs.

b. **Cloud provider.** Person, organization, or entity responsible for making a service available to cloud consumers.

c. **Cloud auditor.** A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.

d. **Cloud broker.** An entity that manages the use, performance, and delivery of cloud services and negotiates relationships between CPs and cloud consumers.

e. **Cloud carrier.** The intermediary that provides connectivity and transport of cloud services from CPs to cloud consumers.

1-4 Cloud Computing Initiatives

Cloud computing has many definitions. The characteristics most interpretations share are as follows:

a. On-demand scalability of highly available and reliable pooled computing resources.

b. Secure access to metered services from nearly anywhere.

c. Displacement of data and services from inside to outside the organization.

While aspects of these characteristics have been realized to some extent, cloud computing remains a "work in progress."

This handbook provides an overview of the security and privacy challenges pertinent to cloud computing and provides considerations the Postal Service must take when implementing a private cloud or public cloud solution.

Cloud initiatives must comply with Postal Service information security policy given in Handbook AS-805, *Information Security,* subchapter 1-6, as follows:

> "Information security policies apply to all information, in any form, related to Postal Service business activities, employees, or customers that have been created, acquired, or disseminated using Postal Service resources, brand, or funding. Information security policies apply to all technologies associated with the creation, collection, processing, storage, transmission, analysis, and disposal of information. Information security policies also apply to all information systems, infrastructure, applications, products, services, telecommunications networks, computer-controlled mail processing equipment, and related resources, which are sponsored by, operated on behalf of, or developed for the benefit of the Postal Service."

1-5 Major Security Objectives for Cloud Computing

The major security objectives for cloud computing are the following:

a. Protect Postal Service data from unauthorized access, disclosure, modification, and monitoring. This includes supporting identity management such that the Postal Service has the capability to enforce identity and access control policies on authorized users accessing cloud services. This also includes the ability of the Postal Service to allow access to its data selectively available to other users.

b. Protect information resources from supply chain threats. This includes verifying and maintaining the trustworthiness and reliability of the CP, as well as the security assurances associated with the hardware and software used.

c. Prevent unauthorized access to cloud computing infrastructure resources. This includes implementing security domains that have a logical separation between computing resources (e.g., logical separation of Postal Service workloads running on the same physical server by virtual machine (VM) monitors [hypervisors] in a multitenant environment) and using default to no-access configurations.

d. Design Web applications deployed in a cloud for an Internet threat model [such as the National Institute of Standards and Technology (NIST)] and embed security into the software development process.

e. Protect Internet browsers from attacks to mitigate end-user security vulnerabilities. This includes taking measures to protect Internet-connected personal computing devices by applying security software, personal firewalls, and patches on a regular maintenance schedule.

f. Deploy access control and intrusion-detection technologies at the CP and conduct an independent assessment to verify that they are in place. This includes, but does not rely on, traditional perimeter security measures in combination with the domain security model. Traditional perimeter security includes: restricting physical access to network and devices; protecting individual components from exploitation through security patch deployment; setting as the default the most secure configurations; disabling all unused ports and services; using role-based access control; monitoring audit trails; minimizing the use of privilege; using antivirus software; and encrypting communications.

g. Define trust boundaries between CPs and consumers to clearly establish and promulgate boundaries of responsibility for providing security.

h. Support portability such that the Postal Service can take action to change CPs when needed to satisfy availability, confidentiality, and integrity requirements. This includes the ability to close an account on a particular date and time and to copy data from one CP to another.

i. Provide physical separation between Postal Service payment card industry (PCI) and non-PCI applications. Postal Service PCI applications cannot share processing and memory storage with non-PCI applications.

2 Roles and Responsibilities

This chapter defines roles and responsibilities for cloud computing.

The executive vice president and chief information officer promotes the protection of information resources in the cloud across Postal Service organizations and business partners.

The chief postal inspector:

a. Investigates cloud computer intrusions and attacks.

b. Investigates the release or attempted release of malicious code in to cloud resources.

The vice president, Information Technology:

a. Implements a secure cloud computing architecture to mitigate information security-related risks.

b. Verifies confidentiality, availability, and integrity of information processed in the cloud.

The vice president, Engineering Systems:

a. Implements a secure cloud computing architecture to mitigate information security-related risks.

b. Verifies confidentiality, availability, and integrity of information processed in the cloud.

The manager, Corporate Information Security Office:

a. Continuously monitors the cloud computing environment to verify the protection of non-publicly available Postal Service information.

b. Conducts certification and accreditation of cloud applications and infrastructure to verify compliance with information security policies and standards.

The officers and managers:

a. Implement information security policies in the cloud.

b. Verify compliance with information security policies by organizations and information resources under their direction and invoke user sanctions as required.

The executive sponsors:

a. Understand the extent of the data protection that a cloud offers (even if limited) and make rational risk-based decisions on when to store data in a cloud.

b. Verify that security requirements are properly addressed and information resources are properly protected in the cloud.

c. Verify that all security requirements associated with clouds are included in contracts and strategic alliances.

d. Involve all stakeholders to include, but not be limited to, Information Technology (IT), Corporate Information Security, and the Privacy Office in the evaluation and procurement of cloud services.

The chief privacy officer:

a. Provides guidance on privacy issues associated with the cloud and verifying Postal Service compliance with the Privacy Act, Freedom of Information Act, Gramm-Leach-Bliley Act, and Children's Online Privacy Protection Act.

b. Develops privacy compliance standards, privacy notice, and data collection standards, including cookies and Web site transfer notifications, for the cloud.

The inspector general:

a. Conducts independent audits and evaluation of the cloud to verify Postal Service assets and resources are fully protected.

b. Detects and reports fraud, waste, and abuse.

c. Investigates cloud computer intrusions and attacks.

d. Investigates the release or attempted release of malicious code to cloud resources.

The contracting officers and contracting officer representatives verify that information technology contractors, vendors, and business partners are contractually obligated to abide by Postal Service information security and privacy policies, standards, and procedures.

The legal officers and legal officer representatives:

a. Provide guidance on legal issues as they apply to applications in the cloud that require a legal hold.

b. Provide guidance on protecting and limiting access to the proprietary architectural, design, and financial information provided to the Postal Service by the CP that is used to determine and monitor the CP’s ability to meet the contract and its security obligations.

3 Cloud Architectures

The architecture of the software and hardware used to deliver cloud services can vary significantly among CPs for any specific service model.

The physical location of the infrastructure is determined by the CP, as is the design and implementation of the reliability, resource pooling, scalability, and other logic needed in the support framework.

Applications are built on the programming interfaces of Internet-accessible services, which typically involve multiple cloud components communicating with each other over application programming interfaces (APIs). Virtual machines typically serve as the abstract unit of deployment for Infrastructure as a Service (IaaS) clouds and are loosely coupled with the cloud storage architecture. CPs may also use other computing abstractions in lieu of virtual machine technology to provide services for other service models.

To complement the server side of the equation, cloud-based applications require a client side to initiate and obtain services. While Web browsers often serve as clients, other possibilities exist.

In addition, an adequate and secure network communications infrastructure must be in place. Many of the simplified interfaces and service abstractions on the client, server, and network belie the inherent underlying complexity that affects security and privacy. Therefore, it is important to understand the technologies the CP uses to provide services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

3-1 Attack Surface

The hypervisor or virtual machine monitor is an additional layer of software between an operating system and hardware platform that is used to operate multi-tenant virtual machines and is common to Infrastructure as a Service (IaaS) clouds. Besides virtualized resources, the hypervisor normally supports other APIs to conduct administrative operations, such as launching, migrating, and terminating virtual machine instances. Compared with a traditional, non-virtualized implementation, the addition of a hypervisor causes an increase in the attack surface. That is, there are additional methods (e.g., APIs), channels (e.g., sockets), and data items (e.g., input strings) an attacker can use to cause damage to the system.

The complexity in virtual machine environments can also be more challenging than in their traditional counterparts, giving rise to conditions that undermine security. For example, paging, check-pointing, and migration of virtual machines can leak sensitive data to persistent storage, subverting protection mechanisms in the hosted operating system intended to prevent such occurrences. Moreover, the hypervisor itself can potentially be compromised. A compromise of the hypervisor could result in the compromise of all systems that it hosts. The Postal Service must maintain a current patch level on all virtual machines.

Virtual servers and applications, much like their non-virtual counterparts, must be secured, both physically and logically. The operating system and applications must be hardened when producing virtual machine images for deployment. Care must also be taken to provide security for the virtualized environments in which the images run. For example, virtual firewalls can be used to isolate groups of virtual machines from other hosted groups, such as production systems from development systems or development systems from other cloud-resident systems. Carefully managing virtual machine images is also important to avoid accidentally deploying images under development or containing vulnerabilities.

3-2 Virtual Network Protection

Most virtualization platforms have the ability to create software-based switches and network configurations as part of the virtual environment to allow virtual machines on the same host to communicate more directly and efficiently. For example, for virtual machines requiring no external network access, the virtual networking architectures of most virtualization software products support same-host networking, in which a private subnet is created for intra-host communications. Traffic over virtual networks may not be visible to security protection devices on the physical network, such as network-based intrusion detection and prevention systems. To avoid a loss of visibility and protection against intra-host attacks, duplication of the physical network protection capabilities may be required on the virtual network.

While some hypervisors allow network monitoring, their capabilities are generally not as robust as those in tools used to monitor physical networks. The Postal Service must consider the risk and performance tradeoffs between having traffic hidden within the hypervisor versus exposing that traffic to the physical network for monitoring. Commercial tools may help in negating this concern.

A side effect of virtualized environments is the potential loss of separation of duties between existing administration roles. For example, in traditional computing environments, computer system administrators typically do not configure network security components, such as intrusion detection and prevention systems and firewalls. Network security administrators, on the other hand, can configure such devices, but typically do not have administrative rights on hosts to grant system access.

In virtual environments, the distinct roles of computer system and network security administrators can collapse into a single role of a virtual infrastructure administrator. Other distinct roles such as that of storage administrators can be similarly affected. Management and operational controls may be needed to compensate for a lack of technical controls in virtual environments for maintaining separation of duty (e.g., computer system administration versus network administration versus database administration). The Postal Service must verify that separation of duties is maintained.

IaaS CPs and manufacturers of virtual machine products maintain repositories of virtual machine images. A virtual machine image entails the software stack, including installed and configured applications, used to boot the virtual machine into an initial state or the state of some previous checkpoint. Sharing virtual machine images is a common practice in some cloud computing environments as a quick way to get started. Virtual machine images created by the Postal Service must be carefully managed and controlled to avoid problems. For instance, images must be kept up to date with the latest security patches. Caution must be taken to avoid using images that have not been vetted or releasing images in a haphazard fashion.

The provider of an image faces risks since an image can contain proprietary code and data and embody vulnerabilities. An attacker may attempt to examine images to determine whether they leak information or provide an avenue for attack. This is especially true of development images that are accidentally released. The reverse may also occur; an attacker may attempt to supply a virtual machine image containing malware to consumers of a cloud computing system. For example, researchers demonstrated that by manipulating the registration process to gain a first-page listing, they could readily entice cloud consumers to run virtual machine images they contributed to the image repository of a popular CP. The risks for consumers running tainted images include theft and corruption of data. The Postal Service must consider implementing a formal image management process to govern the creation, storage, configuration management, protection, and use of virtual machine images.

3-3 Client-Side Protection

A successful defense against attacks requires securing both the client and server side of cloud computing. With emphasis typically placed on the latter, the former can be easily overlooked. Services from different CPs, as well as cloud-based applications developed by the Postal Service, can impose more exacting demands on the client, which may have implications for security and privacy that need to be considered.

Web browsers, a key element for many cloud computing services and the various plug-ins and extensions available for them, are notorious for their security problems. Moreover, many browser add-ons do not provide automatic updates, increasing the persistence of any existing vulnerabilities.

Maintaining physical and logical security over clients can be troublesome, especially with embedded mobile devices such as smart phones. Their size

and portability can result in the loss of physical control. Built-in security mechanisms often go unused or can be overcome or circumvented without difficulty by a knowledgeable party to gain control over the device.

Smart phones are also treated more as fixed appliances with a limited set of functions, than as general-purpose systems. Moreover, cloud applications are often delivered to them through custom-built native applications (i.e., apps) rather than a Web browser. No single operating system dominates smart phones, and security patches and updates for system components are not as frequent as for desktop computers, making vulnerabilities more persistent and widening the window of opportunity for exploitation. As a safeguard, the Postal Service prohibits access to personally identifiable information (PII) and other sensitive data from portable and mobile devices to reduce risk.

The growing availability and use of social media, personal Webmail, and other publicly available sites also have associated risks that are a concern, since they increasingly serve as avenues for social engineering attacks that can negatively impact the security of the browser, its underlying platform, and cloud services accessed. Having a backdoor Trojan, keystroke logger, or other type of malware present on a client, runs counter to protecting the security and privacy of public cloud services, as well as other Internet-facing public services being accessed.

As part of the overall security architecture for cloud computing, the Postal Service must review existing measures and employ additional ones, if necessary, to secure the client side by deploying and allowing access only through hardened browser environments that encrypt network exchanges and protect against keystroke logging.

Security awareness training also is an important measure for the Postal Service to apply, since having individuals adhere to correct practices is an essential safeguard against many types of attacks.

3-4 Cloud Computing Deployment Models

3-4.1 Private Cloud

The private cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

3-4.2 Community Cloud

The community cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

3-4.3 Public Cloud

The public cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the CP.

3-4.4 Hybrid Cloud

The hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (e.g., private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

3-5 Cloud Computing Service Models

Just as deployment models play an important role in cloud computing, service models are also an important consideration. The service model to which a cloud conforms dictates an organization's scope and control over the computational environment and characterizes a level of abstraction for its use. A service model can be actualized as a public cloud or as any of the other deployment models. Three well-known and often-used service models are described in the following sections.

3-5.1 Software as a Service

The Software as a Service (SaaS) model is a model of service delivery where the cloud consumer controls its users and data but not the applications, platforms, and infrastructure. SaaS is the most prevalent service model whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the CP. The cloud consumer does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

3-5.1.1 SaaS Risks

Very limited tools, procedures, or standard data formats or services interfaces exist that could guarantee data and service portability. This makes it extremely difficult for the Postal Service to migrate from one provider to another or migrate data and services to or from the information technology environment. Furthermore, CPs may have an incentive to prevent (directly or indirectly) the portability of the Postal Service services and data. This potential dependency for service provision on a particular CP, depending on the CP's commitments, may lead to a catastrophic business failure should the CP go bankrupt, and the content and application migration path to another provider is too costly (financially or timewise) or insufficient warning is given.

The acquisition of the CP can also have a similar effect, since it increases the likelihood of sudden changes in provider policy and nonbinding agreements such as terms of use (ToU).

3-5.1.2 SaaS Lock-In

Postal Service data will be typically stored in a custom database schema designed by the SaaS provider. Most SaaS providers offer API calls to read (and thereby 'export') data records. However, if the provider does not offer a readymade data 'export' routine, the Postal Service will need to develop a program to extract their data and write it to file ready for import to another provider. A record at one SaaS provider may have different fields than at another provider although there are common underlying file formats for the export and import of data, e.g., XML. The new provider can normally help with this work at a negotiated cost. However, if the data is to be brought back in-house, the Postal Service will need to write import routines that take care of any required data mapping unless the current hosting CP offers such a routine.

Application lock-in is the most obvious form of lock-in (although it is not specific to cloud services). SaaS providers typically develop a custom application tailored to the needs of their target market. The Postal Service may incur very high switching costs when migrating to another SaaS provider as the end-user experience is impacted (e.g., re-training is necessary). Where the Postal Service has developed programs to interact with the provider's API directly (e.g., for integration with other applications), these will also need to be re-written to take into account the new provider's API. In addition, the SaaS provider's application update rate may cause the Postal Service to incur unacceptable re-training costs for the user community.

3-5.2 Platform as a Service

Platform-as-a-Service (PaaS) is a model where the enterprise controls its users, data, and applications, but not the platform and infrastructure. The computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools. The development environment is typically special purpose, determined by the CP and tailored to the design and architecture of its platform. The Postal Service has control over applications and application environment settings of the platform. Security provisions are split between the CP and the Postal Service.

3-5.2.1 PaaS Lock-In

PaaS lock-in occurs at both the API layer (i.e., platform-specific API calls) and at the component level. For example, the PaaS provider may offer a highly efficient back-end data store. Not only must the Postal Service develop code using the custom APIs offered by the provider, but they must also code data access routines in a way that is compatible with the back-end

data store. This code will not necessarily be portable across PaaS providers, even if a seemingly compatible API is offered, as the data access model may be different. PaaS lock-In considerations include the following:

a. PaaS lock-in at the API layer happens as different providers offer different APIs.

b. PaaS lock-in at the runtime layer happens as ‘standard’ runtimes are often heavily customized to operate safely in a cloud environment. For example, a Java runtime may have ‘dangerous’ calls removed or modified for security reasons. The responsibility is on the Postal Services’ developers to understand and take into account these differences.

c. PaaS also suffers from data lock-in, in the same way as in SaaS, but in this case the responsibility is completely on the Postal Service to create compatible export routines.

d. As platform and infrastructure hardware fails and the ability to procure spares diminishes, the Postal Service may have to migrate their applications to the new hardware on a schedule not of their choosing.

3-5.3 Infrastructure as a Service

Infrastructure-as-a-Service (IaaS) is a model where the enterprise controls its users, data, applications, and OS platform but not the underlying virtualization layers and hardware. The basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface. The Postal Service generally has broad freedom to choose the operating system and development environment to be hosted. Security provisions beyond the basic infrastructure are carried out primarily by the Postal Service.

3-5.3.1 IaaS Risks

In using cloud infrastructures, the client necessarily cedes control to the CP on a number of issues which may affect security. For example, ToUs may prohibit port scans, vulnerability assessment, and penetration testing. Moreover, there may be conflicts between Postal Service hardening procedures and the cloud environment. On the other hand, service level agreements (SLAs) may not offer a commitment to provide such services on the part of the CP, thus leaving a gap in security defenses. Moreover, the CP may outsource or sub-contract services to third parties (unknown providers) which may not offer the same guarantees (such as to provide the service in a lawful way) as issued by the CP. Or the control of the CP changes, so the terms and conditions of their services may also change.

3-5.3.2 IaaS Lock-In

IaaS lock-in varies depending on the specific infrastructure services consumed. For example, the Postal Service using cloud storage will not be impacted by non-compatible virtual machine formats. IaaS considerations are as follows:

a. IaaS computing providers typically offer hypervisor based virtual machines. Software and VM metadata is bundled together for portability – typically only within the provider's cloud. Migrating between providers is labor intensive and costly until open standards, such as OVF, are adopted in the future.

b. IaaS storage provider offerings vary from simplistic key/value based data stores to policy enhanced file based stores. Feature sets can vary significantly, therefore so will storage offerings. However application-level dependence on specific policy features (e.g., access controls) may limit the choice of provider.

c. Data lock-in is the obvious concern with IaaS storage services. As the Postal Service pushes more data to cloud storage, data lock-in increases unless the CP provides for data portability.

Common to all providers is the possibility of a 'run on the banks' scenario for a CP. For this scenario, suppose there is a crisis of confidence in the CP's financial position, and therefore a mass exit and withdrawal of content on a first-come, first-served basis. Then, in a situation where a provider limits the amount of 'content' (data and application code) which can be 'withdrawn' in a given timeframe, the Postal Service may never be able to retrieve their data and applications.

Further, a public cloud offers information technology capabilities as a service to any consumer over the public Internet, while a private cloud offers information technology capabilities as a service to a select group of consumers such that access is restricted to increase service attributes (e.g., security). A special kind of a private cloud is an internal cloud: a private cloud by which Postal Service IT provides capabilities as a service in addition to firewalls and security.

4 Cloud Security Concerns and FedRAMP

The three cyber security objectives of confidentiality, integrity, and availability of information and information systems are particularly relevant as these are the high-priority concerns and perceived risks related to cloud computing. Cloud computing implementations are subject to local physical threats as well as remote, external threats. Consistent with other applications, the threat sources include accidents, natural disasters and external loss of service, hostile governments, criminal organizations, terrorist groups, and intentional and unintentional introduction of vulnerabilities through internal and external authorized and unauthorized human and system access, including but not limited to employees and intruders. The characteristics of cloud computing, significantly multi-tenancy and the implications of the three service models and four deployment models, heighten the need to consider data and systems protection in the context of logical as well as physical boundaries.

4-1 Fundamental Security Concerns

4-1.1 System Complexity

A public cloud computing environment is extremely complex compared with that of Postal Service Solution Centers. Many components make up a public cloud, resulting in a large attack surface inside and outside of the United States. Besides components for general computing, such as deployed applications, virtual machine monitors, guest virtual machines, data storage, and supporting middleware, there are also components providing the management backplane for self-service, resource metering, quota management, data replication and recovery, service-level monitoring, workload management, and cloud bursting. Cloud services themselves may also be realized through nesting and layering with services from other CPs across various countries. Components change over time as upgrades and feature improvements occur, confounding matters further.

Security depends not only on the correctness and effectiveness of many components, but also on the interactions among them. Challenges exist in understanding and securing APIs that are often proprietary to a CP. The number of possible interactions between components increases as the square of the number of components, which pushes the level of complexity upward. Complexity typically relates inversely to security, with greater

complexity giving rise to increased vulnerability. Decreases in security also heighten privacy risks related to the unauthorized access, destruction, loss, modification, or disclosure of sensitive and sensitive-enhanced personal data.

4-1.2 Shared Multi-Tenant Environment

Public cloud services offered by CPs have a serious underlying complication — client organizations typically share components and resources with other consumers that are unknown to them. Rather than using physical separation of resources as a control, cloud computing places greater dependence on logical separation at multiple layers of the application stack. While not unique to cloud computing, logical separation is a significant problem that is exacerbated by the scale of cloud computing. An attacker could pose as a consumer to exploit vulnerabilities from within the cloud environment, overcome the separation mechanisms, and gain unauthorized access. Access to Postal Service data and resources could also inadvertently be exposed to other consumers or be blocked from legitimate consumers through a configuration or software error.

Having to share an infrastructure with unknown outside parties is a major drawback for some applications and requires a high level of assurance pertaining to the strength of the security mechanisms used for logical separation.

4-1.3 Internet-Facing Services

Public cloud services are delivered over the Internet, exposing the administrative interfaces used to self-service and manage an account, as well as non-administrative interfaces used to access deployed services. Applications and data that were previously accessed from the confines of the Postal Service intranet must now face increased risk from network threats that were previously defended against at the perimeter of the Postal Service intranet and from new threats that target the exposed interfaces. The performance and quality of services delivered over the Internet may also be at issue.

Relying on remote administrative access as the means for the Postal Service to manage assets that are held within the cloud also increases risk, compared with an Integrated Business Systems Solution Center, where administrative access to platforms can be restricted to direct or internal connections. Similarly, remote administrative access of the cloud infrastructure, if done by the CP, is also a concern. When taken together with the previous two items, a highly complex, multi-tenanted computing environment, whose services are Internet-facing and available to the public, arguably affords a potentially attractive attack surface that must be carefully safeguarded.

4-1.4 Loss of Control

Security and privacy concerns in cloud computing services are amplified by external control over Postal Service assets and the potential for mismanagement of those assets. Transitioning to a public cloud requires a transfer of responsibility and control to the CP over information as well as system components that were previously under Postal Service direct control. The transition is usually accompanied by the lack of a direct point of contact with the

management of operations and influence over decisions made about the computing environment. This situation makes the Postal Service dependent on the cooperation of the CP to carry out activities that span the responsibilities of both parties, such as continuous monitoring and incident response. Compliance with data-protection laws and regulations is another important area of joint responsibility that requires coordination with and the cooperation of the CP.

Loss of control over both the physical and logical aspects of the system and data diminishes the Postal Service's ability to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the Postal Service. Legal protections for privacy may also be affected when information is stored with a third-party CP. Under such conditions, maintaining accountability can be more challenging.

4-2 Federal Risk and Authorization Management Program

The Federal Risk and Authorization Management Program (FedRAMP) supports the U.S. government's objective to enable U.S. federal agencies to use managed service providers that enable cloud computing capabilities.

4-2.1 Overview of FedRAMP Process

FedRAMP allows U.S. federal agencies to make use of CPs platforms and offerings. The FedRAMP program provides an avenue for CPs to obtain a provisional authorization after undergoing a third-party independent security assessment. By assessing security controls on candidate platforms and providing provisional authorizations on platforms that have acceptable risk, FedRAMP enables federal agencies to forego the security assessment process for a multitude of known security controls.

4-2.2 FedRAMP Definition and Purpose

FedRAMP is a governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that will save cost, time, and staff required to conduct redundant agency security assessments.

The purpose of FedRAMP is to:

a. Ensure that cloud-based services used governmentwide have adequate information security.

b. Eliminate duplication of effort and reduce risk management costs.

c. Enable rapid and cost-effective procurement of information systems/services for federal agencies.

FedRAMP uses a security risk model that can be leveraged among agencies based on a consistent security baseline. FedRAMP provides processes, artifacts, and a repository that enables agencies to leverage authorizations with:

a. Standardized security requirements and ongoing cyber security for selected information system impact levels.

b. Conformity assessment program that identifies qualified independent, third-party assessments of security controls implemented by CPs.

c. Standardized contract language to help agencies integrate FedRAMP requirements and best practices into acquisitions.

d. Repository of authorization packages for cloud services that can be leveraged governmentwide.

e. Standardized ongoing assessment and authorization processes for multi-tenant cloud services.

4-2.3 FedRAMP Governance

FedRAMP is governed by a Joint Authorization Board (JAB) that consists of representatives from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense (DoD). The FedRAMP program is endorsed by the U.S. government's Chief Information Officer (CIO) Council including the Information Security and Identity Management Committee (ISIMC). The ISIMC collaborates on identifying high-priority security and identity management initiatives and developing recommendations for policies, procedures, and standards to address those initiatives.

a. JAB performs risk authorization and grants the provisional Authority To Operate (ATO).

b. FedRAMP Program Management Office (PMO) is responsible for operational management.

c. National Institute of Standards and Technology (NIST) provides technical assistance to the Third-Party Assessment Organization (3PAO) process, maintains Federal Information Security Management Act (FISMA) standards, and establishes technical standards.

d. Federal CIO Council coordinates cross agency communications.

e. DHS monitors and reports on security incidents and provides data feeds for continuous monitoring.

4-2.4 High-Level Operations

FedRAMP provides a standardized approach to security assessments and ongoing assessments and authorizations (continuous monitoring) designed to save cost, time, and staff required to assess and authorize cloud services. FISMA requires federal agencies to accept the risk and authorize cloud systems at the agency level. Accordingly, the FedRAMP Policy Memo requires federal agencies to use FedRAMP when assessing, authorizing, and continuously monitoring cloud services in order to aid agencies in this process as well as save government resources and eliminate duplicative efforts.

The FedRAMP security authorization process has four distinct areas (see Exhibit 4-2.4):

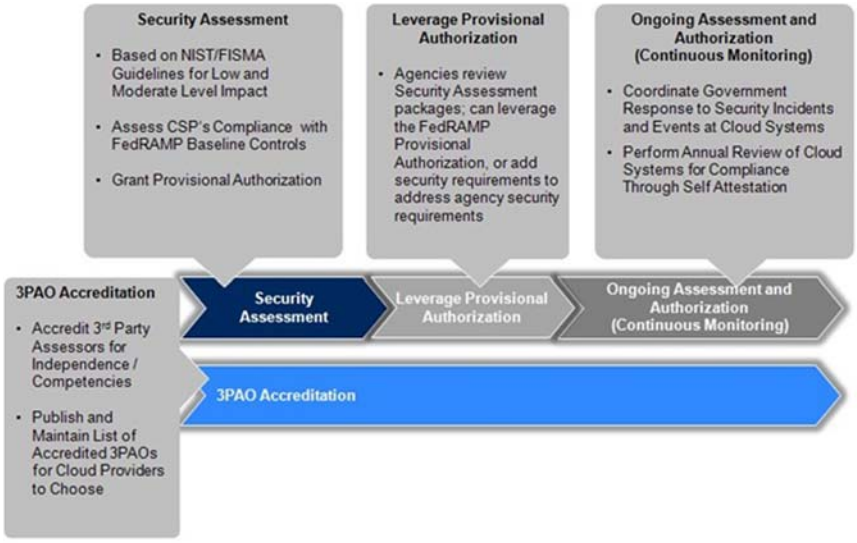
a. Security assessment.

b. Leverage of the ATO.

c. Ongoing assessment and authorization (continuous monitoring).

d. 3PAO accreditation.

Exhibit 4-2.4
FedRAMP Security Authorization Process



4-2.4.1 Security Assessment

A CP or an agency may request a provisional ATO granted by the JAB under the FedRAMP security assessment process. The process follows the NIST 800-37 risk management framework as tailored for a shared responsibility environment. The CP identifies the appropriate baseline; implements appropriate security controls, and documents the implementation. The CP contracts with an accredited 3PAO to independently verify and validate their security implementations and their security assessment package. The CP submits the package to FedRAMP for review. Once documentation and test results are completed, the assessment is measured against the FedRAMP requirements and if the JAB is satisfied that the risks are acceptable, a provisional authorization is granted. Agencies can then leverage the JAB provisional authorization as the baseline for granting their own ATO.

4-2.4.2 Leverage Authority to Operate

The PMO will maintain a repository of FedRAMP provisional authorizations and associated security assessment packages for agencies to review. Agencies can use the provisional authorizations and security assessment packages as a baseline for granting their own ATO. If necessary, agencies can add additional controls to the baseline to meet their particular security profile.

4-2.4.3 Ongoing Assessment and Authorization (Continuous Monitoring)

For systems with a provisional authorization, FedRAMP, in conjunction with DHS, conducts ongoing assessment and authorization (continuous monitoring) activities. Ongoing assessment and authorization (continuous monitoring) determine if the set of deployed security controls continue to be effective over time.

4-2.4.4 Third-Party Assessment Organization Accreditation

CPs applying for an ATO must use an accredited 3PAO. A review board, with representation from NIST and the FedRAMP PMO, accredits 3PAOs. The approval process requires applicants to demonstrate their technical capabilities and their independence as an assessor. The approval process follows the conformity assessment approach outlined in ISO/IEC 17020. FedRAMP maintains a list of approved 3PAO from which CPs can choose.

5 Cloud Risk Management

Risk management is the process of identifying and assessing risk to Postal Service operations, assets, or individuals resulting from the operation of information systems and taking the necessary steps to reduce it to an acceptable level. This process includes the completion of a risk assessment, the implementation of a risk mitigation strategy, and the employment of techniques and procedures for the continuous monitoring of the security state of information systems. Cloud-based systems, as with traditional information systems, require that risks are managed throughout the system lifecycle.

Assessing and managing risk in systems that use cloud services can be a challenge. The Postal Service policy requires external providers handling Postal Service information or operating information systems on behalf of the Postal Service to meet the same security requirements as Postal internal departments. To the maximum extent practicable, the Postal Service must verify that privacy and security controls are implemented correctly, operate as intended, and meet its requirements. The Postal Service must understand the privacy and security controls of the cloud service, establish adequate arrangements in the service agreement, make any needed adjustments, and monitor compliance of the service controls within the terms of the agreement.

5-1 Cloud-Specific Risks

With cloud-based services, some subsystems or subsystem components fall outside of the direct control of the Postal Service. With less control over processes and equipment, the Postal Service is less able to have visibility into the presence of specific risks, weigh alternatives, set priorities, and act decisively.

5-1.1 Loss of Governance

In using cloud infrastructures, the Postal Service necessarily cedes control to the CP on a number of issues which may affect privacy and security. At the same time, SLAs may not ensure appropriate controls are in place to protect data and may not offer a commitment to provide such services on the part of the CP, thus leaving a gap in security defenses.

5-1.2 Lock-In

Currently only a few tools, procedures, standard data formats or APIs, or services interfaces exist that could guarantee data, application, and service portability. This can make it difficult for the Postal Service to migrate from one

provider to another or migrate data and services back to an in-house IT environment. This introduces a dependency on a particular CP for service provision, especially if data portability, as the most fundamental aspect, is not enabled. The use of standard industry protocols will reduce vendor lock-in.

5-1.3 Isolation Failure

Multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants (e.g., so-called guest-hopping attacks). However it should be considered that attacks on resource isolation mechanisms (e.g., against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional operating systems.

5-1.4 Compliance Risks

Achieving certification and accreditation may be put at risk by migration to the cloud:

a. If the CP cannot provide evidence of their own compliance with the relevant requirements.

b. If the CP does not permit audit by the Postal Service.

In certain cases, it also means that using a public cloud infrastructure implies that certain kinds of compliance cannot be achieved (e.g., Payment Card Industry Data Security Standard).

5-1.5 Management Interface Compromise

Management interfaces of a public CP will be accessible through the Internet to mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk, especially when combined with remote access and Web browser vulnerabilities.

5-1.6 Data Protection

Cloud computing poses several data protection risks for the Postal Service and providers. For example, there is limited ability to encrypt data at rest in a multi-tenancy environment. In some cases, it may be difficult for the Postal Service (in its role as data controller) to effectively check the data-handling practices of the CP and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds. On the other hand, some CPs provide information on their data-handling practices. Some CPs also offer certification summaries on their data processing and data security activities and the data controls they have in place.

5-1.7 Insecure or Incomplete Data Deletion

When a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible, either because extra copies of data are stored but are not available, or because the disk to be destroyed also

stores data from other clients. Multiple tenancies and the reuse of hardware resources represent a higher risk to the Postal Service than with dedicated hardware.

5-1.8 Insider Threat

While usually less likely, the damage caused by insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security CPs. Cloud computing insider threats can be unintentional or malicious.

Unintentional insider threats often result from careless entry of administrative commands that negatively affect Postal Service systems, services, and data. However, it can also result from a lack of training in the proper management of Postal Service systems and services.

The principal issue with malicious insider threats is that the attacker is already on the inside. The insider knows the security controls and procedures and has the ability to compromise the confidentiality, integrity, and availability of Postal Service information.

Possible types of intentional attacks include theft of information, data destruction or corruption, damage to systems serving the Postal Service, damage to software and services being used by the Postal Service, plus sabotage and fraud.

Trade secrets, engineering documents, financial data, customer data and many other valuable assets could be copied and sold to the highest bidder or simply distributed anywhere. This could happen with the perpetrator remaining completely invisible.

In data destruction or corruption, insiders can access critical customer files and databases and erase the data, introduce viruses or worms, or introduce logic bombs to damage/erase the data at a future date. If this critical data is not backed up and/or replicated at an alternate location, its loss would be serious for the Postal Service.

Important customer-facing applications may malfunction or not operate at all. This means that the customers may be unable to transact business properly, resulting loss of business and loss of reputation. It may be difficult and even impossible to regain customer trust, especially if damage to customer-facing systems has been severe.

Fraudulent activities can be easily launched within cloud environments. The perpetrator has secure access to multiple customer systems and data and is only limited by his or her computing skills.

Note: In some cases it is advisable for the Postal Service to transfer risk to the CP; however not all risks can be transferred. If a risk leads to serious damage to reputation or legal implications, it is hard or impossible for any other party to compensate for this damage. Ultimately, responsibility can be outsourced but accountability remains the responsibility of the Postal Service.

5-2 Attacks Against Cloud Computing Services

Some scenarios of attacks against cloud computer services include the following:

a. Compromises to the confidentiality and integrity of data in transit to and from a CP.

b. Attacks which take advantage of the homogeneity and power of cloud computing environments to rapidly scale and increase the magnitude of the attack.

c. Unauthorized access by a consumer (through improper authentication or authorization, or vulnerabilities introduced during maintenance) to software, data, and resources in use by an authorized cloud service consumer.

d. Increased levels of network-based attacks, such as denial of service attacks, which exploit software not designed for an Internet threat model and vulnerabilities in resources which were formerly accessed through private networks.

e. Attacks which exploit the physical abstraction of cloud resources and exploit a lack of transparency in audit procedures or records.

f. Attacks that take advantage of virtual machines that have not recently been patched.

g. Attacks which exploit inconsistencies in global privacy policies and regulations.

6 Cloud Computing Security Policy and Requirements

6-1 Security Policy

Information must be protected from unauthorized access, use, disclosure, disruption, modification, or destruction to help ensure integrity, confidentiality, and availability.

6-2 Security Requirements

The Corporate Information Security Office (CISO) will conduct an infrastructure certification and accreditation (C&A) on the CP to assess compliance with the requirements delineated in 6-2.

6-2.1 Cloud Security Providers

CPs must:

a. Be FedRAMP certified.

b. Comply with FISMA Moderate Authorization and Accreditation security controls and processes.

c. Comply with *Payment Card Industry (PCI) Data Security Standard (DSS)* version 2.0 and the *Information Supplement: PCI DSS Cloud Computing Guidelines* if that functionality is provided within the cloud.

6-2.2 Cloud Initiatives

Each cloud initiative must have a design document provided to CISO/Information Technology that contains key infrastructure domains, communication demarcations, and data locations. The diagram(s) must contain, but are not limited to, data flow, computing hardware locations, internal communication protocols, key communication external demarcation locations and data repositories and/or databases. See Handbook AS-805 for further details.

6-2.3 Postal Service Applications and Information

Requirements for Postal Service applications and information are as follows:

a. Sensitive, sensitive-enhanced, and critical applications/information must not be deployed to external clouds, community clouds, or hybrid clouds.

b. Internal private clouds are acceptable for sensitive, sensitive-enhanced, and critical applications/information.

c. Internal private clouds, community clouds, hybrid clouds, and external clouds are acceptable for non-sensitive and non-critical applications/ information with the appropriate AS-805 security controls and specific cloud controls in place to protect the cloud environment.

d. Postal Service information must not be processed or stored outside the contiguous United States (48 states and Washington, D.C.).

6-2.4 Identity Management

A means of integrating Postal Service identity management system with the cloud's identity management solution is required. The user must be authenticated prior to access to cloud applications is provided. Cloud-based applications must be integrated into an identity management framework to avoid separate management of user identities in the cloud. The following actions must be taken:

a. **Single sign-on (SSO).** Upon authentication through the cloud consumer's identity management solution, users should be able to access all cloud services without further authentication.

b. **Strong authentication.** CPs must provide strong authentication using two-factor authentication techniques to support sensitive and critical applications hosted in internal private clouds.

c. **User provisioning.** CPs must deliver standards-based APIs to allow the provisioning of users, either individually or in bulk. As the number of cloud services to which the Postal Service subscribes to increases, the time spent on user maintenance will rapidly increase without the availability of interfaces that allow user management to be automated.

d. **Access policy management.** A standard policy management interface must be implemented under Postal Service control to permit creation, deletion, and maintenance of access policies from a standardized management tool.

6-2.5 Security Audit Information

Security audit data must be maintained for every aspect of the cloud service and defined in the contract, for use in the analysis of security incidents when they are discovered. High-level summaries of security audit information must provide enough information to determine when an event took place, and detailed logs must provide the information needed to perform a forensic analysis of the incident. See Handbook AS-805 for specific audit requirements. Security measures are as follows:

a. **Security audit data retention.** The CP must retain security audit data per Postal Service requirements.

b. **Security audit data monitoring.** The CP must monitor security audit data with the frequency needed to rapidly identify and respond to security incidents, and notify the Postal Service promptly in the event of a security breach.

c. **Periodic vulnerability scans.** The CP must perform vulnerability scans, as defined in the contract, with the results available to the Postal Service on request.

d. **Continual monitoring.** The CP must continually monitor systems to detect and remediate denial-of-service attacks, malware, and other attempts to breach system and data/database security.

e. **Security audit data segregation.** The CP must segregate log data applicable for each client and provide it to each respective client for analysis without exposing log data from other clients.

f. **Security audit data correlation.** Additionally, the ability to maintain an accurate and complete audit trail may require logs from all levels of the infrastructure, requiring involvement from both the CP and the Postal Service. For example, the CP could manage system-level, operating-system, and hypervisor logs, while the Postal Service configures logging for their own VMs and applications. In this scenario, the ability to associate various log files into meaningful events would require correlation of Postal Service-controlled logs and those controlled by the CP.

6-2.6 Encryption

Encryption is required for sensitive and sensitive-enhanced data, both at rest and in transit, to meet security requirements. Sensitive and sensitive-enhanced data must be encrypted using FIPS 140-2–validated encryption modules. Keys must be managed separately from data and require higher privileges. Encryption keys must be changed every two years for sensitive data and annually for sensitive-enhanced data, decrypting data with the old key and re-encrypting the data with the new key. Encryption requirements are as follows:

a. **Encryption of data at rest.** Encryption must be used for sensitive and sensitive-enhanced information stored or archived on fixed and removable devices and media.

b. **Encryption of data in transit.** Encryption of data in transit protects data, including usernames and passwords, from interception. This is especially important when using untrusted network environments.

6-2.7 Physical Security

Postal Service security standards apply to the physical security of the facilities used to house the equipment and services. Physical security includes all measures whose purpose is to prevent physical access to a building, resource, or stored information. The following practices must be followed:

a. **Inspection of premises.** The CP must make all facilities involved in providing the cloud service available for routine site security reviews (SSRs) by the designated Postal Service Inspection Service personnel.

b. **Physical data center location.** The CP must limit the facilities in which the Postal Service's data reside to the contiguous United States including any contingency or archival backup facilities.

6-2.8 Certification and Accreditation

The CP must work with the Postal Service to obtain certification and accreditation that the service being provided meets the requirements of the Postal Service Information Security Certification and Accreditation (C&A) process.

6-2.9 Data Security

Data security must encompass the following:

a. **Data acquisition.** End-to-end processes and data flows must be documented across both the Postal Service and CP networks, so that it is clearly understood where cardholder data is located and how it is traversing the infrastructure.

b. **Data storage and persistence.** In addition to the known range of intended storage locations, data may also be present in other CP systems used for maintenance of the cloud infrastructure. Cardholder data stored in memory could also be written to disk for recovery or high-availability purposes (for example, in the case of virtual machine suspension or snapshot). Such stored data may easily be "forgotten" and so not protected by data security controls. All potential capture points must be identified and managed as necessary to prevent unintended or unsecured storage or transmission of sensitive data. Specialized tools and processes may be needed to locate and manage data stored on archived, off-line, or relocated images. Potential hypervisor access to data in memory must also be taken into consideration to ensure that client-defined access controls are not unintentionally bypassed by the CP administrator personnel.

c. **Data lifecycle management.** Clear requirements for data retention, storage, and secure disposal must be delineated to ensure sensitive and sensitive-enhanced information is:

   (1) Retained for as long as needed.

   (2) Not retained any longer than needed.

   (3) Stored only in appropriate and secured locations.

   (4) Accessible only to those with a business need.

   (5) Handled in accordance with Postal Service security policy.

   (6) Destroyed in accordance with the Postal Services policy and not recoverable upon completion of the destruction process.

d. **Data deletion.** Verifying that data are completely deleted decreases the likelihood of security breaches in the future and keeps the Postal Service compliant with security and privacy statutes. In the cloud, the Postal Service must rely on the CP to delete data from all components (such as hard disks and tapes) including contingency or archival backups. Deletion policies are as follows:

   (1) **Deletion of Postal Service data at the termination of a contract.** The CP must return all Postal Service data and provide evidence that the data is irrevocably deleted from all of their

systems (including contingency and archival backups). The CP must provide documentation attesting to such deletions.

(2) **Deletion of logs, usage data, and audit data at the termination of a contract.** The CP must delete all logs, usage data, and audit data from all services that could be traced back to the Postal Service or its users.

(3) **Attestation of how the CP will comply.** The CP must provide an attestation of how they will comply with the requirements for deletion of Postal Service data.

6-2.10 Continuity of Operations of CP

The continuity of operations of a CP entails the following:

a. **Code escrow.** To protect the Postal Service from a CP exiting the market place, declaring bankruptcy, or de-supporting a cloud solution and to support the ability of the Postal Service to set up this solution with another CP, the CP must put a copy of the current version and all subsequent versions of non-COTS source code required to recreate the system in escrow within the contiguous United States at the CP's expense.

b. **Cloud environment.** The CP must provide the ability to rapidly recreate the environment if a CP is no longer able to provide access to the current instance of the system. This includes the development environment with all the necessary hardware, system software, compilers, and quality assurance tools.

c. **Attestation of how the CP will comply.** The CP must provide an attestation of the how the CP will comply with the requirements for continuity of operations.

6-2.11 Architecture

Architecture used by the CP must include the following:

a. The underlying technologies and technical controls that the CP uses to provide services, including the security and privacy of the system across all system components must be documented and available for review by the Postal Service.

b. Visibility must be provided into the security and privacy controls and processes employed by the CP and their performance over time.

c. Sensitive and sensitive-enhanced databases and file repositories in an internal private cloud must be monitored with database activity monitoring and file activity monitoring to identify instances of large data migrations.

d. Employee, business partner, and supplier Internet access must be monitored with URL filtering and/or data loss prevention (DLP) tools to identify actions associated with sensitive and sensitive-enhanced data moving to external, community, or hybrid clouds.

e. DLP must be used to identify sensitive and sensitive-enhanced data leaking from internal private cloud deployments.

f. When moving files and their metadata to a new cloud environment, copies of file metadata must be securely removed to prevent metadata information from remaining behind.

g. Access control and intrusion detection/intrusion prevention technologies must be installed to provide continuous monitoring of the cloud environment.

6-2.12 Governance, Risk, and Compliance

The policies related to governance, risk, and compliance are as follows:

a. Postal Service policies, procedures, and standards used for application design, development, testing, implementation, use, and monitoring must be extended to the cloud.

b. Virtualization and other logical isolation techniques that the CP employs in its multi-tenant software architecture must be assessed to understand the risks to the Postal Service. The assessment must be documented and available for review by the Postal Service.

c. An independent assessment must be conducted by a qualified third party to verify that Postal Service information is protected in the cloud environment.

d. The CP risk management program must address the constantly evolving and shifting cloud risk landscape for the lifecycle of the system.

e. The security state of the information system must be continuously monitored to support ongoing risk management decisions.

f. Audit mechanisms and tools must be put in place to ensure Postal Service information is protected throughout the system lifecycle.

g. The CP's electronic discovery capabilities and processes must not compromise the privacy or security of Postal Service data and applications.

6-2.13 Access Management

Access management policies include the following:

a. Clear, exclusive ownership rights over data must be established.

b. Individuals employed with the CP with physical or logical access to sensitive or sensitive-enhance data must be properly vetted via a background investigation and rescreened every 2 years to ensure trustworthiness.

c. Authorization, authentication, and other identity and access management functions must be implemented.

d. The CP's ability to control access to data must be evaluated for suitability to the Postal Service.

e. The risk of collocating Postal Service data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value must be evaluated.

f. The technical ability to protect data varies widely depending on how the data is accessed. A number of access scenarios are possible, including the following:

(1) **In transit to or from a provider.** Data that the Postal Service wishes to upload into a cloud must be protected in transit; similarly, data that the Postal Service wishes to download from a cloud must be protected in transit.

(2) **Passively stored with no shared access.** Data to be accessed only by the Postal Service must be protected against access attempts by all other entities.

(3) **Passively stored with selective shared access.** Data to be accessed only by entities that have been authorized by the Postal Service for specific access modes (e.g., read, write, delete) must be protected against access attempts by unauthorized entities or accesses in unauthorized modes, while preserving availability for authorized entities.

(4) **Passively stored public access.** Data to be accessible anonymously in some authorized modes (e.g., read) but not in other modes except by authorized entities must be appropriately protected.

(5) **Actively processed.** Data to be accessed by a computing application running in a cloud (e.g., a VM, PaaS, or SaaS), but not otherwise to be shared (or shared only selectively) must be appropriately protected.

(6) **Account termination.** Data to be maintained for a fixed period of time must be protected at rest and then purged.

(7) **Deletion.** Postal Service data must be destroyed in accordance with Handbook AS-805.

6-2.14 Availability of Postal Service Applications and Information

Policy related to availability of Postal Service applications and information is as follows:

a. Availability, data backup and recovery, and disaster recovery must meet the Postal Service's continuity and contingency planning requirements to ensure that all operations can be reinstituted in a timely and organized manner following an intermediate or prolonged disruption.

b. Although the migration of a service or application to a cloud environment may provide some inherent level of redundancy, executive sponsors must verify that contingency and disaster recovery plans are documented and available for review by the Postal Service.

6-2.15 Incident Response

Incident response policy is as follows:

a. Security breaches must be detected and remediated in a timely manner.

b. Procedures for incident detection, remediation, and response must be documented and available for review by the Postal Service.

c. The response process must be in place and sufficient mechanisms in place to share information during and after an incident such that the Postal Service can respond to incidents in a coordinated fashion with the CP in accordance with their respective roles and responsibilities.

d. The Postal Service needs to know when an issue, incident, or breach has occurred and the impact to their environment and/or to their data. Issues, incidents, and data breaches must be communicated by the CP in a timely manner. The Postal Service must consider whether their CP requires all clients to immediately notify the CP of potential breaches in their environments, allowing the CP to respond more quickly to contain the breach and minimize its impact to other clients.

e. Definitions of what constitutes a breach or incident requiring notification between the Postal Service and the CP must be agreed upon. Notification processes and timelines must be included in SLAs, and incident response plans must include notification requirements. The potential for Postal Service data to be captured by third parties during a breach investigation should also be clearly understood.

f. Investigating potential breaches in cloud environments brings additional challenges. For example, compromised VM instances may be deactivated before anyone is aware that a breach has occurred. It may be nearly impossible to properly investigate a breach when the source of the breach is no longer in use or even exists.

6-2.16 Application Security

The policy related to application security is as follows:

a. Data storage must be dispersed for redundancy where possible.

b. All sensitive and sensitive-enhanced data moving to an internal private cloud, within the cloud network layer, or at nodes before network transmission must be encrypted, including all service and deployment models.

c. A content discovery tool must be used to scan cloud storage and identify unencrypted sensitive and sensitive-enhanced data in an internal private cloud.

d. When using application encryption, encryption keys must be stored externally to the application. Encryption keys must be escrowed and maintained locally.

e. APIs and other software interfaces are an integral component of cloud computing, supporting interoperability and rapid delivery of cloud services. APIs must be configured to provide access to a variety of functions, allowing the Postal Service and CPs to interact and manage their interactions within the cloud service.

f. As Web services and APIs are by nature publicly accessible, their security is critical to the security of the resources they provide access to. If not properly developed, managed, and secured, these interfaces can be exploited or compromised, resulting in unexpected behavior and potentially unauthorized access. For example, a poorly-coded API could result in weak authentication protocols, poor access controls, and limited auditing capability. Such weaknesses could lead to the exposure of authentication credentials and other sensitive data. If the APIs are not properly secured, they could also be exploited or altered by an attacker to redirect data flows or alter application behavior.

g. APIs and other public interfaces must be designed to prevent both accidental misuse and malicious attempts to bypass security policy. Strong authentication and access controls, strong cryptography, and real-time monitoring are examples of controls that must be in place to protect these interfaces.

h. Security Assurance Markup Language (SAML) or Web Service Security (WSS) must be used for authentication so the controls can be interoperable with other standard-based systems.

i. Trust boundaries between CP(s) and consumers must be defined to clearly establish and promulgate the boundaries of responsibility for providing security.

6-2.17 Administrative Security

Administrative security policy is as follows:

a. Access privileges must be audited and reconfirmed for system administrators and technicians semiannually.

b. Prospective system administrators and technicians who may have access to Postal Service systems and data must have background checks. Background checks must be updated every 5 years. Individuals with criminal records must be subject to further scrutiny or removed from consideration altogether.

c. System administrators and technicians must complete initial and ongoing security training and acknowledge in writing that they have completed the training.

d. System administrators and technicians must demonstrate their competence through careful questioning or professional certifications.

e. System administrators and technicians must be trained on the current systems in use and acknowledge in writing that they have completed the training.

f. Nontechnical employees must be trained annually and acknowledge in writing that they have completed the training.

g. Are malicious acts by insiders documented? This is probably one of the most important issues to address when evaluating prospective CPs; it should be part of any request for proposal and the CP should submit documented evidence of the incident. Although this question may be considered company confidential, a nonresponse to this issue should raise a major red flag.

h. Has a CP employee ever been convicted of insider attacks on customers? Again, be prepared for a sanitized or nonresponse as it may be a sensitive issue to the CP and its position may be to keep it confidential. However, a reputable cloud service firm should be willing to own up to its mistake and describe how an incident helped it improve its security policies and practices.

6-2.18 IaaS Security

IaaS security policy is as follows:

a. Security testing must be conducted to verify the infrastructure is performing as designed.

b. Sensitive and sensitive-enhanced volumes in an internal private cloud must be encrypted to limit exposure. The unauthorized creation of snapshots or unapproved administrator access could result in data misuse.

c. VM images must be de-provisioned after an application is ported from the CP.

d. Controls must be in place to support decommissioning of disk and storage devices in the cloud.

e. Access must be granted to system logs, traces, and access and billing records from the legacy CP to verify data integrity and charges incurred for a specific period of time.

f. Management-level functions, interfaces, or APIs being used must be compatible with or implemented by the new CP.

g. CISO must be provided a list of authorized individuals with access to the encryption keys.

6-2.19 PaaS Security

PaaS security policy is as follows:

a. Security testing must be completed prior to and after the cloud migration to verify the services or applications are operating correctly.

b. Sensitive and sensitive-enhanced data in applications and storage in an internal private cloud must be encrypted.

c. Security tools must be available for secure data transfer, backup, and restore.

d. Security protection (e.g., access control, encryption, and intrusion detection and prevention systems) must be available for data placed into the cloud and for data generated and maintained in the cloud.

e. CP and user responsibilities for testing must be documented and communicated to all stakeholders.

6-2.20 SaaS Security

SaaS security policy is as follows:

a. Security testing must be conducted to verify the software is performing as designed.

b. Regular data extractions and backups must be conducted in a format that is usable without the SaaS CP.

c. Periodic reviews and audits must be conducted to verify the consistency and effectiveness of controls across old and new CPs.

6-2.21 Multi-Tenancy

In a multi-tenant cloud environment, client organizations generally have no knowledge of the other clients with whom they share resources (for example, virtual infrastructure and data stores) or how other clients are securing (or not securing) their environments that access the shared resources.

Whether unsavory clients can pose a risk to other clients using the same provider will largely depend on the controls the CP has in place to segregate clients from one another and to monitor and detect suspicious activity on the shared infrastructure and between client environments. Before engaging with a CP, the Postal Service must consider how the CP verifies that their clients are who they say they are, and how the CP detects potentially suspicious behavior once the clients are onboard. The Postal Service must also ask the CP what controls they have in place to verify that the security posture of one client cannot affect the security posture of another client.

6-2.22 Due Diligence

The Postal Service must follow a thorough due-diligence process prior to engagement of the CP including:

a. Confirming the CP has a history of sound work practices and ethical behavior.

b. Verifying that the CP is compatible with the Postal Service's business image and risk profile.

c. Identifying potential risks or circumstances associated with the CP that may impact Postal Service operations or business.

d. Identifying elements of the service that need to be clarified, and that need to be included in contracts or service agreements.

Due diligence is not simply reading the CP's marketing material or relying on their claims of secure operations. The Postal Service must be sufficiently assured that they are engaging with a CP that can meet their security and operational needs before undertaking any such engagements.

This page intentionally left blank

7 Legal Considerations

7-1 Contract Clauses

Certain standard contract clauses may deserve additional review because of the nature of cloud computing. Pay particular attention to rights and obligations relating to notifications of breaches in data security and data privacy, data storage locations, data transfer, creation of derivative works, change of control, and access to data by law enforcement entities. Because the cloud can be used to outsource critical internal infrastructure, and the interruption of that infrastructure may have wide ranging effects, pay attention to whether the standard limitations of liability adequately represent allocations of liability, given the parties' usage of the cloud, or the allocation of responsibilities for infrastructure.

The following is a list of areas the Postal Service should pay particular attention to when assessing SLAs, ToUs, user licensing agreements (ULAs), and other agreements for cloud services:

a. **Data protection.** Give attention to choosing a CP that provides sufficient technical security measures and organizational measures governing the processing to be carried out and documenting compliance with those measures.

b. **Data security and data privacy.** Give attention to mandatory data security and data privacy measures that potentially cause either the CP or the Postal Service to be subject to regulatory and judicial measures if the contract does not address these obligations.

c. **Data storage locations.** Give attention to ensure that Postal Service information resides in the contiguous United States.

d. **Data transfer.** Give attention to what information is provided to the Postal Service regarding how data is transferred within the CP's proprietary cloud and outside that cloud as well as between any geographically different CP sites.

e. **Law enforcement access.** Each country and state has unique restrictions on and requirements providing for law enforcement access to data. The Postal Service should pay attention to information available from the provider about the jurisdictions in which data may be stored and processed and evaluate any risks resulting from the jurisdictions which may apply.

f. **Confidentiality and non-disclosure.** Review the duties and obligations related to this issue.

g. **Intellectual property.** In the case of IaaS and PaaS, intellectual property, including original works created using the cloud infrastructure, may be stored. The Postal Service must confirm that the contract respects their rights to any intellectual property or original works as far as possible without compromising the quality of service offered (e.g., backups may be a necessary part of offering a good service level).

h. **Risk allocation and limitation of liability.** When reviewing their respective contract obligations, the parties should underscore those obligations that present significant risk to them by including monetary remediation clauses, or obligations to indemnify, for the other party's breach of that contract obligation. Furthermore, any standard clauses covering limitations of liability must be evaluated carefully.

i. **Change of control.** Verify there is transparency concerning the CP's continuing ability to honor their contract obligations in the case of a change of control, as well as any possibility to terminate the contract.

j. **Compliance with applicable laws and regulations.** The cloud environment must be compliant with all applicable laws and regulations including other procurement and acquisition requirements such as, but not limited to, compliance with Section 508 of the Rehabilitation Act of 1973.

7-2 Electronic Discovery

Electronic discovery involves the identification, collection, processing, analysis, and production of electronically stored information (ESI) in the discovery phase of litigation. The Postal Service has other obligations to preserve and produce electronic documents, such as complying with audit and regulatory information requests and complying with Freedom of Information Act (FOIA) requests. ESI includes not only electronic mail, attachments, and other data objects stored on a computer system or storage media, but also any associated metadata, such as dates of object creation or modification, and non-rendered file content (i.e., data that is not explicitly displayed for consumers).

The capabilities and processes of a CP, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the Postal Service to meet its obligations in a cost effective, timely, and compliant manner.

For example, a CP's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation. The CP's electronic discovery capabilities and processes must not compromise the privacy or security of the data and applications of the Postal Service in satisfying the discovery obligations of other cloud consumers, and vice versa.

7-3 Data Ownership

The Postal Service ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved. Ideally, the contract should state clearly that the Postal Service retains exclusive ownership over all its data; that the CP acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the Postal Service data for its own purposes; and that the CP does not acquire and may not claim any interest in the data due to security.

7-4 Data Mining

The CP must not analyze Postal Service data anonymously and use it for their purposes or share it with third parties.

7-5 Privacy

The privacy of individuals and their personally identifiable information (PII)[1], that is collected, used, maintained, shared, and disposed of by programs and information systems, must be protected by the Postal Service. Privacy also involves each individual's right to decide when and whether to share personal information, how much information to share, and the particular circumstances under which that information can be shared. The privacy of individuals depends on the safeguards employed within the information systems that are processing, storing, and transmitting PII and the cloud environments in which those systems operate. The Postal Service cannot have effective privacy without a strong foundation of information security by the CP.

1. PII is information that can be used to identify an individual. The definition of PII is not anchored to any single category of information. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified by examining the context of use and combination of data elements. In performing this assessment, it is important to recognize that non-PII can become PII, whenever additional information is made publicly available, in any medium and from any source that, when combined with other available information, could be used to identify an individual.

This page intentionally left blank

8 Legal, Privacy, and Information Security Contract Requirements

8-1 Background Questions for Contract

The key background questions to ask the CP relative to contracts are the following:

1. In what country is the CP located?
2. Is the CP's infrastructure located in the same country or in different countries?
3. Will the CP use other companies whose infrastructure is located outside that of the CP?
4. Where will the data including contingency and archival backups be physically located?
5. Will jurisdiction over the contract terms and over the data be divided?
6. Will any of the CP's services be subcontracted out?
7. Will any of the CP's services be outsourced?
8. How will the data provided by the Postal Service and their customers be collected, processed, and transferred?
9. What happens to the data sent to the CP upon termination of the contract?
10. What happens to the data upon sale or transfer of the CP to another entity?
11. What happens to the data if the CP declares bankruptcy?

8-2 Legal Requirements

The contract must address the following:

a. All CPs must be FedRAMP certified.

b. The CP's headquarters must be located in the contiguous United States.

c. The CP's infrastructure must be located in the contiguous United States.

d. If the CP uses other companies to provide services (i.e., subcontracted out or outsourced), the infrastructure associated with those services must be located in the contiguous United States.

e. Postal Service data, including backups, must be physically located in the contiguous United States.

f. Jurisdiction over contract terms must not be divided.

g. Jurisdiction over Postal Service data must not be divided.

h. CP subcontractors, including outsourcing providers, must comply with contract terms established between the Postal Service and the CP.

i. Data provided by the Postal Service and their customers must be collected, processed, and transferred in accordance with the contract terms established between the Postal Service and the CP.

j. The contract must provide for ending the relationship with the CP upon request, termination of the contract, or declaration of bankruptcy by the CP. Once the relationship with the CP has ended, Postal Service information must be returned or transferred to another CP, and all Postal Service information ruminates left on the CP's equipment must be appropriately destroyed.

k. Information must be provided by the CP about the jurisdictions in which data may be stored and processed and any risks resulting from the location of those jurisdictions must be evaluated.

l. The contract must respect Postal Service rights to any intellectual property or original works without compromising the quality of service offered.

m. Backups must be provided as part of the service offering.

n. The contract must delineate how costs and responsibilities will be apportioned for containing and mitigating a breach.

o. The contract must define the procedures and payment responsibilities for notification to individuals if a breach of sensitive or sensitive-enhanced information occurs.

p. The contract must define how the costs for credit monitoring will be apportioned.

q. The disposition of Postal Service data and software if the provider declares bankruptcy. Postal Service data could become an asset in the bankruptcy proceedings.

   (1) Procedures for the transfer of Postal Service data must be defined.

   (2) The current version and all subsequent versions of the software implemented by the CP must be escrowed in the United States at the CP's expense to protect the code in the event the CP declares bankruptcy.

r. The disposition of Postal Service data and software if the provider is sold to or acquired by another entity.

   (1) Procedures for the transfer of Postal Service data must be defined.

   (2) The current version and all subsequent versions of the software implemented by the CP must be escrowed in the United States at the CP's expense to protect the code in the event the CP is sold to or acquired by another entity.

8-3 Privacy Contract Requirements

The contract must address the following:

a. The location of all servers, including back-up servers, must be in the contiguous United States. Data stored outside the United States cannot be protected under the Privacy Act and may allow for certain local or foreign law enforcement authorities to search Postal Service data pursuant to a court order, subpoena, or informal request outside the control of the Postal Service.

b. The permitted use of the information which the CP collects:

   (1) Controls must be established around the CP's ability to analyze or search the data for their own purposes or to sell to third parties.

   (2) Postal Service data cannot be used for purposes other than the purposes agreed upon with the Postal Service.

c. Data retention periods.

d. The procedure for purging records at the end of the retention period. If the procedure is not automated, the frequency of purging must be defined and the date of each purge must be documented for audit purposes.

8-4 Information Security Contract Requirements

The contract must address the following:

a. The frequency of data back-ups.

b. The offsite location for storage of data backups. The offsite location must not be subject to the same threats.

c. Procedures must be defined to ensure Postal Service data is not comingled with the data from other organizations.

d. Procedures for handling incidents must be defined to include the following:

   (1) Notification to the Postal Service.

   (2) Cost and responsibility for containing or mitigating harm.

   (3) Postal Service or CP notification of individuals if their personal information was disclosed.

   (4) Postal Service or CP payment for the notification.

   (5) Postal Service or CP payment for credit monitoring.

e. System security requirements must be defined.

f. Audit rights must be defined. If the provider moves data, the Postal Service could lose rights and access to conduct audits.

g. Access controls must be defined and the following should be defined:
   (1) The Postal Service and CP rights to access the data.
   (2) Security clearances of those with access.
   (3) The privacy and security training to be provided.

h. Data loss prevention software to be implemented. Will the Postal Service existing software work if the software is moved to the cloud?

Appendix A

Analysis for Cloud Deployment

Criterion	Question	Guidelines
Criticality	Does the candidate application provide business critical functions?	■ Mission-critical candidates should be deployed on premise or in a private cloud ■ Mission candidates should be avoided until organizational cloud capabilities are more mature, e.g., there is more organizational experience and institutional knowledge
Complexity	How complex is the candidate application, in terms of architecture, interfaces, and configuration, for migration to the cloud?	■ Don't move legacy applications (e.g., mainframe, j2EE) to the cloud unless extensive reengineering is planned in the near future ■ High complexity candidate applications should be deployed in a cloud
Cost	Is there a significant cost reduction opportunity? If so, how much?	■ Target candidate applications with the highest cost savings ■ Costs should never be the primary criteria for the cloud migration
Variability	How much variability exists or is possible between baseline and peak for a given timeframe (e.g., predictable and unpredictable demand variations, on-off processes, critical or seasonal loads)?	■ High variability candidate applications should be moved to a cloud unless there are risk, compliance, or mission criticality issues
High Performance	Does this candidate application require huge computing resources to process structured and/or unstructured data?	■ Candidate applications with high-performance needs should be move to a cloud unless there are risk, compliance, or mission criticality issues
New Capability	Does the cloud provide a new capability that can better support business goals?	■ Candidate applications where a private cloud provide a significant new capability should be move to a cloud unless there are risk, compliance, or mission criticality issues
Speed to Market	Is the speed to market for the capability to which the candidate application is associated critical?	■ Use the inherent benefit "speed to market" of cloud computing from the cloud provider
Security, privacy, and compliance	Does the candidate application pose security, privacy risk or is the application bound by regulations or industry requirements	■ Candidate applications with increased security, privacy, or compliance requirements should be avoided until organizational cloud capabilities are more mature ■ When feasible, Candidate applications with increased security, privacy, or compliance requirements should be deployed to a private cloud

This page intentionally left blank

Appendix B

Cloud Terms and Definitions

Term	Definition
Cloud Access	To make contact with or gain access to a cloud Provider.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance, and delivery of cloud services and negotiates relationships between CPs and cloud consumers.
Cloud Carrier	The intermediary that provides connectivity and transport of cloud services between CPs and cloud consumers.
Cloud Consumer	The person or organization that maintains a business relationship with and uses service from CPs.
Cloud Distribution	The process of transporting cloud data between CPs and cloud consumers.
Cloud Provider (CP)	Person, organization, or entity responsible for making a service available to service consumers. Also known as cloud service provider.
Cloud Service Management	Includes all the service-related functions that are necessary for the management and operations of those services required by or proposed to customers.
Community Cloud	The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
Data Portability	The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported.
Fixed Endpoints	A physical device, fixed in its location that provided a man/machine interface to cloud services and applications. A fixed endpoint typically uses one method and protocol to connect to cloud services and applications.
Hybrid Cloud	The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).
Information Security	Includes protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: a. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; b. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; c. Availability, which means ensuring timely and reliable access to and use of information.

Term	Definition
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
Interoperability	The capability to communicate, to execute programs, or to transfer data among various functional units under specified conditions.
Metering	Provide a measuring capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).
Mobile Endpoints	A physical device, often carried by the user that provided a man/machine interface to cloud services and applications. A mobile endpoint may use multiple methods and protocols to connect to cloud services and applications.
Monitoring and Reporting	Discover and monitor the virtual resources, monitor cloud operations and events, and generate performance reports.
Performance Audit	Systematic evaluation of a cloud system by measuring how well it conforms to a set of established performance criteria.
Physical Resource Layer	Includes all the physical resources used to provide cloud services, most notably, the hardware and the facility.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
Portability	The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported and the ability of software or of a system to run on more than one type or size of computer under more than one operating system.
Privacy	Provides for the proper and consistent collection, processing, communication, use, and disposition of disposition of personal information (PI) and personally-identifiable information (PII) throughout its life cycle.
Privacy Impact Assessment (PIA)	Systematic evaluation of a cloud system by measuring how well it conforms to a set of established privacy criteria. The PIA is integrated in the Postal Service Business Impact Assessment (BIA) process.
Private Cloud	The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
Provisioning/Configuration	The process of preparing and equipping a cloud to allow it to provide (new) services to its users.
Public Cloud	The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
Rapid Provisioning	Automatically deploying cloud system based on the requested service/ resources/capabilities.
Resource Abstraction and Control Layer	Entails software elements, such as hypervisor, virtual machines, virtual data storage, and supporting software components, used to realize the infrastructure upon which a cloud service can be established.
Resource Change	Adjust configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud.

Term	Definition
Security Assertion Markup Language (SAML)	The set of specifications describing security assertions that are encoded in XML; profiles for attaching the assertions to various protocols and frameworks; the request/response protocol used to obtain the assertions; and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP). SAML addresses Web single sign-on, Web services authentication, attribute exchange, authorization, non-repudiation, and secure communications. SAML defines assertion message formats that are referenced in Liberty Alliance, Shibboleth, WS-Security, and other specifications. SAML has become the standard Web SSO identity management solution. Several versions have been released to date, including SAML 1.0, SAML 1.1, and SAML 2.0. The Organization for the Advancement of Structured Information Standards (OASIS) oversees SAML.
Security Audit	Systematic evaluation of a cloud system by measuring how well it conforms to a set of established security criteria.
Service Aggregation	An aggregation brokerage service combines multiple services into one or more new services. It will ensure that data is modeled across all component services and integrated as well as ensuring the movement and security of data between the service consumer and multiple providers.
Service Arbitrage	Cloud service arbitrage is similar to cloud service aggregation. The difference between them is that the services being aggregated aren't fixed. Indeed the goal of arbitrage is to provide flexibility and opportunistic choices for the service aggregator, e.g., providing multiple e-mail services through one service provider or providing a credit-scoring service that checks multiple scoring agencies and selects the best score.
Service Consumption	A cloud broker in the act of using a cloud service.
Service Deployment	All of the activities and organization needed to make a cloud service available.
Service Intermediation	An intermediation broker provides a service that directly enhances a given service delivered to one or more service consumers, essentially adding value on top of a given service to enhance some specific capability.
Service Interoperability	The capability to communicate, execute programs, or transfer data among various cloud services under specified conditions.
Service Layer	Defines the basic services provided by CPs.
Service Orchestration	Refers to the arrangement, coordination, and management of cloud infrastructure to provide different cloud services to meet IT and business requirements.
Service Provision	A cloud broker in the act of providing a cloud service.
Service Level Agreement Management	Encompasses the contract definition (basic schema with the quality of service parameters), monitoring, and enforcement, according to the defined policies.
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
System Portability	The ability of a service to run on more than one type or size of cloud.
Web Services Security (WS-Security or WSS)	A flexible and feature-rich extension to SOAP to apply security to Web services. It is a member of the WS-* family of Web service specifications published by OASIS. The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as SAML, Kerberos, and X.509. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security.

This page intentionally left blank

Appendix C

Cloud Acronyms

Acronym	Description
3PAO	Third-Party Assessment Organization
API	Application Programming Interface
ATO	Authority To Operate
CIO	Chief Information Officer
CISO	Corporate Information Security Office
CP	Cloud Provider
DAM	Database Activity Monitoring
DHS	Department of Homeland Security
DoD	Department of Defense
DSS	Data Security Standard
ESI	Electronically Stored Information
FAM	File Activity Monitoring
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
IaaS	Infrastructure as a Service
ISIMC	Information Security and Identity Management Committee
JAB	Joint Authorization Board
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PCI	Payment Card Industry
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
PMO	Program Management Office
SaaS	Software as a Service
SAML	Security Assurance Markup Language
SLA	Service Level Agreement
SSO	Single Sign-On
SSR	Site Security Review
ToU	Terms of Use
ULA	User Licensing Agreement
VM	Virtual Machine
WSS	Web Service Security

This page intentionally left blank

Appendix D

References

1. NIST SP 500-291, Cloud Computing Standards Roadmap, July 2011
2. NIST SP 500-292, Cloud Computing Reference Architecture, September 2011
3. NIST SP 500-293, US Government Cloud Computing Technology Roadmap Volume 1, High-Priority requirements to Further USG Agency Cloud Computing Adoption, Release 1 Draft
4. NIST SP 500-293, US Government Cloud Computing Technology Roadmap Volume II, Useful Information for Cloud Adopters, Release 1 Draft
5. NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing
6. NIST SP 800-145, The NIST Definition of Cloud Computing, *http://csrc.nist.gov/publications*
7. Cloud Security Alliance, The Cloud Control Matrix
8. NIST SP 800-146, Cloud Computing Synopsis and Recommendations (Draft)
9. Proposed Security Assessment & Authorization for U.S. Government Cloud Computing
10. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
11. Top Threats to Cloud Computing V1.0
12. NIST Cloud Computing Security Impediments and Mitigations List
13. SaaS, PaaS, and IaaS: a Security Checklist for Cloud Models
14. Cloud – 10 Risks with Cloud IT Foundation Tier

This page intentionally left blank