Contents

1 Introduction

Cloud computing focuses on leveraging current technologies, information security safeguards, alignment of business objectives and responsibilities, infrastructure, risk mitigation, legal and contractual obligations, privacy requirements, integrated with the exchange and sharing of Postal Service data, and information resources.

1-1 Purpose

The purpose of this handbook is to outline Postal Service policies, standards and requirements that apply to the use of cloud technologies, not addressed in the AS-805, *Information Security*. Information covered in this handbook also includes mitigating security controls for conditions under which cloud technologies can be implemented as cost-effective, risk-based alternative processes.

1-2 Handbook Contents and Policy Owner

Business and administrative objectives, roles and responsibilities, contract obligations, risk management and legal obligations related to cloud technologies are included in the following chapters:

a. Chapter 1: Introduction.
b. Chapter 2: Roles and Responsibilities.
c. Chapter 3: Cloud Architectures.
d. Chapter 4: Cloud and Security Concerns.
e. Chapter 5: Cloud Risk Management.
f. Chapter 6: Cloud Technology Security Requirements.
g. Chapter 7: Legal Considerations.
h. Chapter 8: Legal, Privacy and Information Security Contract Requirements.

The policy owner of this handbook is the Chief Information Security Officer. Send questions and comments to *information_security@usps.gov*.

1-3 Cloud Security Background

Cloud technologies leverage the economies of scale and resource-balancing activities across an ecosystem of partners that include cloud service providers, data brokers and other relevant role players.

Cloud technologies potentially run the risk of minimizing trust and confidence that customers have grown to expect from the Postal Service™ with respect to processing and protecting personal information. The challenge for the Postal Service is to maintain and sustain the confidence level of its customers, while ensuring a chain-of-trust across the architecture and legal structures that are established with cloud providers (CPs).

Exhibit 1 represents an overview of cloud technology architecture, which identifies the major cloud components and their functions in cloud technology.

The high-level cloud conceptual technology model below defines five major components: cloud consumer, cloud provider, cloud carrier, cloud auditor and cloud broker. Each component is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud technology.

Exhibit 1
The Conceptual High-Level Model

The five major components are defined as follows:

a. **Cloud Consumer:** A **p**erson or organization that maintains a business relationship with, and uses service from Cloud Providers.

b. **Cloud Provider:** A **p**erson, organization, or entity (also frequently referred to as cloud service provider) that is 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 Cloud Providers and Cloud Consumers.

e. **Cloud Carrier:** The intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

1-4 Supporting References

The following handbook and management instruction provide additional implementation policy for this handbook:

a. Handbook AS-805, *Information Security,* is the overarching information security document.

b. Management Instruction AS-800-2014-4, *Cloud Computing Policy*, outlines the processes and procedures that must be followed for all technology product and service solutions that use cloud computing

technology. As with any project requiring technology support, business customers must initiate a conversation with their Business Relationship program manager using a documented Business Needs Statement.

1-5 Cloud Technology Initiatives

Cloud technology can and does mean different things to different people. The common characteristics most interpretations share are: on-demand scalability of highly available and reliable pooled technology resources, secure access to metered services from nearly anywhere and displacement of data and services from inside to outside the organization. While aspects of these characteristics have been realized to a certain extent, cloud technology remains a "work in progress."

This document provides an overview of the security and privacy challenges pertinent to cloud technology and points out considerations the Postal Service should take when implementing a private cloud or public cloud environment.

Cloud initiatives must comply with Postal Service information security policy delineated in Handbook AS-805, section 1-6.2.3.

1-5.1 Cloud Solution

"A cloud solution enables network access to a shared pool of configurable virtualized technology resources (e.g., networks, servers, storage, applications and services) in which information technology-enabled capabilities are delivered "as a service" to multiple customers using the same technology resources. The cloud environment can be rapidly scaled up or down and tailored to serve multiple consumers on demand with minimal management effort or service provider interaction.

1-5.2 Hosted Solutions and Service-Based Contracts

Cloud solutions must not be confused with the following:

a. Hosted solutions that are managed and maintained by the supplier and provide physical separation of the hardware that is leased, purchased or isolated for the exclusive use of Postal Service.

b. Service-based contracts where the supplier takes ownership and full responsibility for the security of the data.

1-6 Major Security Objectives for Cloud Technology

The major security objectives for cloud technology are as follows:

a. Protect Postal Service information from unauthorized access, disclosure, modification or 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 make access to its data selectively available to other users.

b. Protect Postal Service information from supply chain threats, including ensuring the trustworthiness and reliability of the service provider.

c. Prevent unauthorized access to cloud technology infrastructure resources.

d. 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.

e. Define trust boundaries between CP(s) and consumers to ensure that the responsibility for providing security is clear.

f. 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, to copy data from one CP to another and then have the data completely purged from the prior CP resources.

2 Roles and Responsibilities

All officers, business and line managers and supervisors, regardless of functional area, are responsible for implementing information security policies. All officers and managers must ensure compliance with information security policies by organizations and information resources under their direction and provide personnel, financial and physical resources required to appropriately protect information resources.

This chapter defines the roles and responsibilities for cloud technology. See Handbook AS-805 for a complete list of roles and responsibilities.

2-1 Chief Inspector

The chief inspector is responsible for:

a. Investigating cloud computer intrusions and attacks.

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

2-2 Executive Vice President and Chief Information Officer

The Executive Vice President and Chief Information Officer is responsible for promoting the protection of information resources in the cloud across Postal Service organizations and business partners.

2-3 Vice President, Information Technology

The vice president, Information Technology, is responsible for:

a. Implementing secure cloud technology architectures to mitigate associated information security-related risks.

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

2-4 Vice President, Chief Information Security Officer

The vice president, Chief Information Security Officer, is responsible for:

a. Continuous monitoring of the cloud technology environment to ensure the protection of non-publicly available Postal Service information.

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

2-5 Executive Sponsors

Executive sponsors are responsible for:

a. Understanding the extent of the data protection that a cloud offers and making rational risk-based decisions on when to store data in a cloud.

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

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

2-6 Chief Privacy Officer

The Chief Privacy Officer is responsible for:

a. Providing guidance on privacy issues associated with the cloud to ensure Postal Service compliance with the Privacy Act of 1974, Freedom of Information Act, Gramm-Leach-Bliley Act, Children's Online Privacy Protection Act, and other concerns as defined in Handbook AS-353, Guide to Privacy, the Freedom of Information Act, and Records Management and the USPS Privacy Policy.

b. Developing privacy compliance standards, Privacy Act Statements, privacy notices, and data collection standards, including cookie usage and website transfer notifications, for the cloud.

2-7 Inspector General

The Inspector General is responsible for:

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

b. Detecting and reporting fraud, waste, and abuse in the cloud.

c. Investigating cloud computer intrusions and attacks.

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

2-8 Contracting Officers and Contracting Officer Representatives

Contracting officers and contracting officer representatives are responsible for ensuring that information technology contractors, suppliers, vendors and business partners are contractually obligated to abide by Postal Service information security and privacy policies, standards, and procedures.

2-9 Manager, Business Relationship Management

The manager, Business Relationship Management, manages all cloud services, including the establishment and maintenance of an enterprise-wide inventory of all cloud technologies.

This page intentionally left blank

3 Cloud Architectures

The architecture of software and hardware used to deliver cloud services can vary significantly among CPs for any specific service model. See the *Postal Service Cloud Computing Enterprise Architecture* on the IT Web site for additional information.

The CP determines the physical location of an infrastructure, 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 cloud storage architecture. CPs may also use other technology abstractions in lieu of virtual machine technology to provision 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 technologies the CP uses to provision 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 Cloud Technology Models

Private cloud: This 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.

Community cloud: This 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.

Public cloud: This 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.

Hybrid cloud: This cloud infrastructure is a composition of two or more distinct cloud infrastructures (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).

3-2 Cloud Technology Service Models

Just as deployment models play an important role in cloud technology, 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 3-2.1, 3-2.2, and 3-2.3.

3-2.1 Software as a Service (SaaS)

SaaS applies when the enterprise controls its users and data, but not the applications, platforms and infrastructure.

SaaS is a model of service delivery in which 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.

Risks: There is currently little in the way of tools, procedures or standard data formats or services interfaces that could guarantee data and service portability. This makes it extremely difficult for the Postal Service to change from one provider to another, or migrate data and services to another CP, or back to the Postal Service IT 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 on a particular CP 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 time-wise) or insufficient warning for required action is given.

The acquisition of the CP by another CP or entity can also have a similar effect, since it increases the likelihood of sudden changes in provider policy and non-binding agreements such as terms of use (ToU).

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 CP offers such a routine.

Application lock-in: This 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. As a result, the Postal Service may incur very high switching costs when changing to another SaaS provider because the end-user experience is impacted (e.g., re-training may be necessary). Where the Postal Service has developed programs to interact with the providers 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.

3-2.2 Platform as a Service (PaaS)

PaaS applies where the enterprise controls its users, data and applications but not the platform and infrastructure.

Platform-as-a-Service (PaaS) is a model of service delivery where the technology 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.

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 at the API layer happens as different providers offer different APIs.
- 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 Service's developers to understand and take into account these differences.

- 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.

3-2.3 Infrastructure as a Service (IaaS):

IaaS applies where the enterprise controls its users, data, applications, OS platform but not the underlying virtualization layers and hardware.

IaaS is a model of service delivery where the basic technology 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.

Risks: In using cloud infrastructures, the client necessarily cedes control to the CP on a number of issues which may affect security. For example, a ToU may prohibit port scans, vulnerability assessments and penetration testing. Moreover, there may be conflicts between Postal Service hardening procedures and the cloud environment. On the other hand, 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 CP may be acquired by another company, so the terms and conditions of their services may change.

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

- 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 IT capabilities as a service to any consumer over the public Internet, while a private cloud offers IT 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.

This page intentionally left blank

4 Cloud Security Concerns

Three key cyber security objectives: ensuring confidentiality, integrity and availability of information resources and systems are high-priority concerns and potential risks to cloud technology. The implementation of cloud technology is subject to local physical threats as well as remote, external threats. Consistent with other IT applications, threat sources include accidents, natural disasters, external loss of service, hostile governments, criminal organizations, terrorist groups, intentional and unintentional vulnerabilities through internal/external authorized and unauthorized system access, including but not limited to employees, contractors, vendors and intruders. The characteristics of cloud technology, specifically multi-tenancy and implications of three service and four deployment models, heighten the efforts to protect Postal Service data and systems, as well as physical boundaries.

The fundamental security concerns associated with cloud deployments are:

a. **System Complexity:** A public cloud technology environment is extremely complex when compared with that of Postal Service IT 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 technology, such as deployed applications, virtual machine monitors, guest virtual machines, data storage and supporting middleware, there are also components providing 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.

b. **Shared Multi-tenant Environment:** Public cloud services offered by providers 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, public cloud technology places greater dependence on logical separation at multiple layers of the application stack. While not unique to cloud technology, logical separation is a significant problem that is exacerbated by the scale of cloud technology. 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.

   Multi-tenancy and shared resources are defining characteristics of cloud technology. 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).

c. **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 are held within the cloud also increases risk, compared with a Postal Service IT Center, where administrative access to platforms can be restricted to direct or internal connections. Similarly, remote administrative access of cloud infrastructure, if done by the CP, is also a concern. When paired together with the previous two items, a highly complex, multi-tenanted technology environment, whose services are Internet-facing and available to the public, arguably affords a potentially attractive attack surface that must be carefully safeguarded.

d. **Loss of Control:** Security and privacy concerns in cloud technology are amplified by external control over Postal Service assets and the potential for mismanagement of those assets. Transitioning to a public cloud requires transferring responsibilities and direct control over information, as well as system components, from the Postal Service to the CP. The transition is usually accompanied by the lack of a direct point of contact within cloud management operations, and influence

over decisions made about the technology environment. This situation makes the Postal Service dependent on 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 that governs data privacy is another important area of joint responsibility that requires collaboration between the Postal Service and CP.

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

This page intentionally left blank

5 Cloud Risk Management

Assessing and managing threats and risk in systems that use cloud services can be challenging. The Postal Service requires external providers handling Postal data and/or information resources or operating systems to meet the same security standards and requirements as internal users. To that extent, the Postal Service must ensure that privacy and security controls and safeguards are implemented with maximum operational functionality and meet baseline privacy and security requirements as established by FedRAMP and NIST 800-53. The Postal Service understands these requirements and will employ risk mitigation strategies, conduct risk management assessments and provide adequate contract language to ensure compliance with FedRAMP requirements for baseline controls, FedRAMP continuous monitoring and privacy and security requirements and standards. Cloud-based systems, as with traditional information systems, require that risks are managed throughout the system lifecycle. This task will remain an integral part of our risk management process.

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 diminished control over processes and equipment, the Postal Service has limited involvement when making decisions relative to CP environment, due to loss of control.

Loss of Governance: In using cloud infrastructures, the Postal Service formally surrenders 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.

Lock-In: There are currently only a few tools, procedures, standard data formats or APIs or services interfaces that could guarantee data, application and service portability. This can make it difficult for the Postal Service to transfer 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.

Compliance Risks: The application, certification and accreditation (C&A) and CP selection process can create potential risks for the Postal Service, if either of the following is true:

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

b. 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).

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.

Data Protection: Cloud technology 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 will provide information on their data handling practices. Some CPs will also offer certification summaries on their data processing and data security activities and the data controls they have in place.

Insecure or Incomplete Data Deletion: When a request to remove a resource from the cloud 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. As part of day-to-day operations, data storage may not be appropriately wiped prior to reassignment to other cloud customers. Multiple tenancies and the reuse of hardware resources represent a higher risk to the Postal Service than with dedicated hardware.

Malicious Insider: While less likely, the damage caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers.

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 potential 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, some responsibility can be outsourced but accountability remains the responsibility of the Postal Service.*

5-2 Attacks Against Cloud Technologies

Some of the more common attacks against cloud technologies are:

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 technology environments to rapidly scale and increase the magnitude of the attack.

c. Unauthorized access by application users or customers (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.

This page intentionally left blank

6 Cloud Technology Security Requirements

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

6-1 Cloud Providers and Security

The following must apply to cloud providers:

a. Cloud providers must be FedRAMP certified. Exceptions will be reviewed by the CIO on a case-by-case basis.

b. Cloud providers must comply with FISMA Moderate and/or High Authorization and Accreditation security controls and processes.

c. Cloud providers must comply with the current version of the *Payment Card Industry (PCI) Data Security Standard (DSS)* and the *Information Supplement: PCI DSS Cloud Computing Guidelines* if that functionality is provided within a Private Cloud.

6-2 Cloud Initiatives

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

6-3 Administrative Security

The following standards apply to administrative security:

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.

c. System administrators and technicians must complete initial and annual information security training and provide written acknowledgement of completion.

d. System administrators and technicians must demonstrate their competency by responding to appropriate technical knowledge, skills and abilities (KSAs) or acquiring professional certifications.

e. System administrators and technicians must be trained on current systems in use and provide written acknowledgement of completion.

f. Non-technical employees must complete the appropriate annual Postal Service training and provide written acknowledgement of completion.

g. The CP and its employees with access to Postal Service data, systems, and networks must sign non-disclosure agreements.

6-4 Postal Service Applications and Information

The following items apply to Postal Service applications and information:

a. Sensitive, sensitive-enhanced and critical applications/information must not be deployed to External Clouds, Community Clouds, or Hybrid Clouds without the proper controls.

b. Internal Private Clouds (provided by a CP at Postal Service facilities) are acceptable for sensitive, sensitive-enhanced and critical applications/information.

c. Internal Private Clouds (provided by a CP at Postal Service facilities), Community Clouds, Hybrid Clouds and External Clouds are acceptable for Non-Sensitive and Non-Critical applications/information with the appropriate Handbook AS-805 security controls and specific cloud controls in place to protect the cloud environment.

d. Postal Service information may only be processed or stored by a CP within the United States or the U.S. territories.

6-5 Identity Management

A means of integrating identity management in the cloud 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 items apply:

a. **Single Sign-On (SSO).** Upon authentication through the cloud consumer's identity management solution, users must 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.

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. **Background Checks.** Individuals employed with the CP with physical or logical access to sensitive or sensitive-enhance data must be properly vetted and screened periodically (at least every 5 years) to ensure trustworthiness.

e. **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.

6-6 Security Audit Information

Security audit data must be maintained (for every aspect of cloud service) and defined in the contract, for use in the analysis of security incidents when they are discovered. The following items apply to security audits:

a. **Security Audit Log Contents.** 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.

b. **Security Audit Data Retention.** The CP must retain security audit data per Postal Service requirements.

c. **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.

6-7 Encryption

Encryption is required for all Postal Service data, both at rest and in transit, to meet security requirements. The following items apply to encryption:

a. **Encryption of Data at Rest.** Encryption must be used for all Postal Service data 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.

c. **Implementation Requirements.** All Postal Service 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 on a regular basis, decrypting data and re-encrypting with the new key.

6-8 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 items apply to physical security:

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 continental United States including any contingency or archival backup facilities.

6-9 Infrastructure and Application Assessment and Authorization

The CP must work with the Postal Service to ensure that the service being provided meets the requirements of the Postal Service Information Resource Certification and Accreditation (C&A) Process.

6-10 Multi-Tenancy

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

Whether unsavory clients can pose a risk to other clients using the same provider will largely depend on 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 which controls they have in place to verify that the security posture of one client cannot affect the security posture of another.

6-11 Data Deletion

Ensuring that data is completely deleted decreases the likelihood of security breaches in the future and ensures the Postal Service is meeting security and privacy guidelines, policies and statutes. In the cloud, the Postal Service must rely on the CP to ensure deletion of all data from appropriate

components (such as hard disks and tapes) including contingency or archival backups. The following items apply to deletion of data:

a. **Deletion of Postal Service Data at the Termination of a Contract.** The CP must return all Postal Service data and ensure that data is irrevocably deleted from all of their systems (including contingency and archival backups).

b. **Deletion of Logs, Usage Data, and Audit Data at the Termination of a Contract.** The CP must delete all logs, and usage and audit data from all services that could be traced back to the Postal Service or its users.

c. The CP must provide attestation of how the CP will comply with the requirements (e.g., wiping, degaussing and cross-cut shredding) for deletion of Postal Service data.

6-12 Continuity of Operations of CP

The following items apply to continuity of operations:

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 the source code required to re-create the system in escrow within the continental United States at the CPs expense.

b. **Cloud Environment.** The CP must provide the ability to rapidly re-create the exact same operating environment if the CP is no longer able to provide access to the current instance of the system.

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

6-13 Architecture

The following items apply to architecture:

a. The underlying technologies and technical controls that CP uses to provision services, including the security and privacy of systems across all system components must be documented.

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 must be monitored with Database Activity Monitoring (DAM) and File Activity Monitoring (FAM) to identify instances of large data migrations in the cloud.

d. Employee 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 the cloud.

e. DLP must be used to identify any and all sensitive and sensitive-enhanced data leaking from 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 continually deployed by the CP.

6-14 Governance, Risk and Compliance

The following items apply to governance, risk and compliance:

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 documented and assessed to understand all potential risks to the Postal Service.

c. An independent assessment must be conducted to verify that the cloud environment is secure.

d. The risk management program must be adapted to 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 on-going risk management decisions.

f. Audit mechanisms and tools must be put in place to ensure Postal Service practices are followed 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.

6-15 Data Access Management

The following items apply to data access management:

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

b. Adequate safeguards must be in place to secure authentication, authorization, and other identity and access management functions.

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

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

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

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

(2) **Passively stored with no shared access:** Data that should be accessed only by the Postal Service must be encrypted.

(3) **Passively stored with selective shared access:** Data that should 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 that should be accessible anonymously in some authorized modes (e.g., read), should not be accessed in other modes except by authorized entities.

(5) **Actively processed:** Data that is accessed by computing applications running in a cloud (e.g., a VM, PaaS, or SaaS), but that may not be shared and/or may be shared with authorized entities.

(6) **Account Decommission or Retirement:** Data that should be maintained for a predetermined fixed period of time.

(7) **Deletion:** The authorized erasure of Postal Service data.

6-16 Availability of Postal Service Applications and Information

The following items apply to the availability of Postal Service applications and information:

a. The CP contract provisions and procedures for availability, data backup, restoration, and disaster recovery must meet the Postal Service's continuity and contingency planning requirements to ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.

b. Although the migration of a service or application to a cloud environment may provide some inherent level of redundancy, executive sponsors must ensure that contingency and disaster recovery plans are documented.

6-17 Incident Response

The following items apply to incident response:

a. Contract provisions and procedures for incident response and breaches must be understood to ensure that they meet the requirements of the Postal Service.

b. The CP must have a transparent response process in place and sufficient mechanisms to share information during and after an incident or breach to ensure that the Postal Service can respond to incidents and breaches in a coordinated fashion with the CP in accordance with their respective roles and responsibilities.

6-18 Application Security

The following items apply to application security:

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

b. All Postal Service data moving to, 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.

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

e. Open and published APIs (APIs) must be used to ensure the broadest support for interoperability between components, and to facilitate migration of applications and data between CPs.

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

g. Trust boundaries between service provider(s) and consumers must be defined to ensure that the responsibility for providing security is clear.

6-19 Infrastructure as a Service (IaaS)

The following items apply to Iaas:

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

b. All Postal Service volumes must be encrypted to limit exposure. The unauthorized creation of snapshots or unapproved administrator access could result in data misuse.

c. Virtual Machine (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 within 24 hours 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.

6-20 Platform as a Service (PaaS)

The following items apply to PaaS:

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

b. All Postal Service data in applications and storage must be encrypted.

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

d. Security protection must be available for data placed, generated, and maintained in the cloud.

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

6-21 Software as a Service (SaaS)

The following items apply to SaaS:

a. Security testing must be conducted to ensure 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 ensure the consistency and effectiveness of controls across old and new CPs.

6-22 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 reviewing 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 the Postal Service's security and operational needs before undertaking any such engagements.

7 Legal Considerations

7-1 Contract Clauses

Information security clauses must be included in cloud computing contracts. In addition, other standard contract clauses may deserve additional review because of the nature of cloud technology. Pay particular attention to rights and obligations relating to notifications of breaches in data security and data privacy, data storage locations, data transfers, creation of derivative works, change of ownership or 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 CP's 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 Service Level Agreements (SLAs), ToUs, User License Agreements (ULAs) and other agreements for cloud services:

a. **Data Protection**: Choose a CP that provides sufficient technical security measures and organizational measures governing processing procedures and ensuring compliance with those measures.

b. **Data Security and Data Privacy**: Mandatory data security and data privacy measures that potentially cause the CP or Postal Service to subjective regulatory and judicial measures if the contract does not address these obligations.

c. **Data Storage Locations**: Ensure sensitive, sensitive-enhance and critical information resides in the United States or U.S. territories.

d. **Data Transfer**: Information provided to the Postal Service regarding how data is transferred within, internally and externally, the CP's proprietary cloud.

e. **Law Enforcement Access**: Each country has unique restrictions and requirements allowing law enforcement to access data. Understanding what information is available from CPs regarding jurisdictions where data may be stored and processed, and evaluating potential risks within those jurisdictions are critical for risk mitigation.

f. **Confidentiality and Non-disclosure**: Duties and obligations related to maintaining confidentiality and adherence to the terms of the non-disclosure agreement.

g. **Intellectual property**: Intellectual property, including original works created using the cloud infrastructure, may be stored. The Postal Service must ensure that the CP contract respects the Postal Services' right 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**: Underscore the respective contract obligations that present significant risk to the Postal Service (include any monetary remediation clauses or obligations to indemnify) and breach of the CP contract obligations. Furthermore, review and evaluate any standard clauses covering limitations of liability.

i. **Change CP Ownership**: Transparency concerning the CP's continuing ability to honor its contract obligations in the case of a change of ownership or control, as well as any possibility to rescind the contract.

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 Privacy

The privacy of individuals and their personally identifiable information[1] (PII) that is collected, used, maintained, shared and disposed of by programs and information systems must be protected by the Postal Service and suppliers working on behalf of 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. Therefore, the Postal Service maintains industry best practices by ensuring that each CP provide a strong foundation of information security safeguards to protect PII within their cloud environment.

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:

a. In what country is the CP located?

b. What is the name of the data protection authority for that country?

c. Is the CP's infrastructure located in the same country or in different countries?

d. Will the CP use other companies whose infrastructure is located outside that of the CP?

e. Where will the data including contingency and archival backups be physically located?

f. Will jurisdiction over the contract terms and over the data be divided?

g. Will any of the CP's services be subcontracted out?

h. Will any of the CP's services be outsourced?

i. How will the data provided by the Postal Service and their customers be collected, processed, and transferred?

j. What happens to the data sent to the CP upon termination of the contract?

k. What happens to the data upon sale or transfer of the CP to another entity?

l. 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 United States (or U.S. territories).

c. The CP's infrastructure must be located in the United States (or U.S. territories).

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 United States (or U.S. territories).

e. Postal Service data, including backups, must be physically located in the United States or U.S. territories).

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. Data sent to the CP must be returned to the Postal Service upon request, termination of the contract, or declaration of bankruptcy by the CP.

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.
   (3) Procedures for removal of data remnants must be defined.

8-3 Privacy Contract Requirements

The contract must address the following:

a. If the supplier operates a system of records on behalf of the Postal Service, the Privacy Act of 1974 (5 U.S.C. 522a), the Postal Service regulations at 39 CFR Parts 266–267, and Handbook AS-353, Guide to Privacy, the Freedom of Information Act, and Records Management and Appendix, apply to those records. The supplier is required to protect and safeguard customer and employee information from unauthorized access and disclosure.

b. If the supplier has access to Postal Service information pertaining to individuals (e.g. customer or employee information), including address information, whether collected online or offline by the Postal Service or by a supplier acting on its behalf, the supplier must comply with all requirements listed in Clause 1-1 Privacy Protection.

c. The location of all servers, including back-up servers, must be in the United States (or U.S. territories). Data stored outside the United States cannot be protected under the Privacy Act of 1974 or safe harbor framework, 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.

d. 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.

e. Data retention periods.

f. 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 and breaches must be defined to include:

   (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 provider moves data, the Postal Service could lose rights and access to conduct audits.

g. Access controls must 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 that will be provided.

   (4) Encryption methods.

h. Data loss prevention software to be implemented. Assurance that existing software will operate effectively in the cloud?

Appendix 1

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.
Federal Risk and Authorization Management Program (FedRAMP)	A government wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services designed to save cost, time, and staff required to assess and authorize cloud services. The purpose of FedRAMP is to: ensure that cloud-based services used government-wide have adequate information security; eliminate duplication of effort and reduce risk management costs; and enable rapid and cost-effective procurement of information systems/services for federal agencies. FedRAMP provides processes, artifacts, and a repository that enables agencies to leverage authorizations with: standardized security requirements and ongoing cyber security for selected information system impact levels; conformity assessment program that identifies qualified independent, third-party assessments of security controls implemented by CPs; standardized contract language to help agencies integrate FedRAMP requirements and best practices into acquisitions; repository of authorization packages for cloud services that can be leveraged government-wide; and standardized ongoing assessment and authorization processes for multi-tenant cloud services.
Hosted Solution	Infrastructure that is managed and maintained by a supplier to provide physical separation of the Postal Service from the suppliers other customers. The hardware and software is for the exclusive use of Postal Service whether it is leased or purchased.

Term	Definition
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).
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental technology 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).
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.
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.
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.
Service-Based Contracts	The supplier takes ownership and full responsibility for the security of the Postal Service's data.
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 email). 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.