Cloud Security Guidance

.gov Cloud Security Baseline

28 February 2018

Version 0.2

Homeland Security

Table of Contents

I. INTRODUCTION

Approach

Purpose
This document will articulate a cloud computing security baseline to be considered as federal Agencies acquire commercial cloud computing services. This document is intended to help Agencies understand and address the risks and challenges associated with securing their data and applications in a commercial cloud environment by providing a foundational cloud data security reference point.

Scope
This document is intended to serve as a foundational data security reference point, or baseline, for federal agencies transitioning to the commercial cloud. This document is not intended to represent federal government cloud architecture. This cloud security baseline draws upon four basic cloud security capability elements:

1. Agency use cases that describe the data security features leveraged by federal agencies that are using, or plan to use, the commercial cloud. This element of the baseline includes only the information provided by the use case Agency.
2. Cloud security guidelines and recommendations described in open-source literature, such as NIST or FedRAMP that address known or theorized cloud security concerns or considerations that have the potential to impact cloud data security.
3. Cloud security guidelines and recommendations found in public-private sources such as the Cloud Security Alliance.
4. Cloud security recommendations, affirmations, and observations as determined by the Department of Homeland Security's Network Security Deployment organization's .govCAR efforts, and how they link to other elements of the baseline.

The cloud security baseline is based on prevailing cloud security guidance documentation, analyses of currently available technologies, and known best practices across government and industry. The security recommendations and guidelines in this document promote concepts that enhance data security, while recognizing that data security cannot be guaranteed.

Mission
This document will leverage existing standards and guidelines, build out additional security measures that address growing cloud risks, and provide new baseline guidance for .gov for the commercial cloud.

Guiding Principles
Guiding Principles reflect strategic choices affecting the development and implementation of the cloud security guidance baseline.

1. **Engage the stakeholder community in the development and the implementation of the cloud security guidance.** Cloud security is a community-wide effort involving a broad range of stakeholders. A collaborative approach to engaging the community will

create opportunities to capture the diversity of requirements and missions across the stakeholder community.

2. **Build on existing policy.** Recent Administrations have produced policies related to the evolution of federal IT, including the transition to the cloud. The cloud security guidance will leverage, where possible, these existing standards, policies, and governance mechanisms, and augment them only as needed to address the challenges of the cloud environment.

3. **Emphasize public commercial cloud services.** Cloud options vary, from private and on-premises to public, commercial configurations. Security approaches articulated in this document will be designed for the public commercial cloud.

4. **Emphasize risk-informed choices when prioritizing.** Stakeholder resources are limited, requiring prioritization of security approaches. As appropriate, prioritization choices will be made that are risk-informed and depend on the sensitivity level of the data being secured and on the risk tolerance of the Agency.

5. **Aim for a capability portfolio that spans the stakeholder community.** The capability portfolio will address capabilities across the breadth of the stakeholder community, encompassing all stakeholders that can deliver and implement security capabilities.

II. CLOUD SECURITY GUIDANCE BASELINE

Baseline Cloud Security Architecture

In an ideal .gov cybersecurity scenario, an authoritative cloud reference architecture would be created as a guiding architectural model for federal agencies as a security foundation to build upon as they transition data and applications to a commercial cloud environment. However, due to the variety of commercial cloud service providers (CSPs) and cloud service models, a wide diversity in data security needs and requirements across federal agencies, and a quickly evolving cloud computing technical environment, any individual reference architecture would soon be obsolete once created. In contrast, a cloud security "baseline" of recommended cloud security capabilities framed from existing guidance, knowledge of cloud security risks, use cases in which an Agency is already in the process of leveraging the commercial cloud, and on threat-based government cybersecurity capability assessments can provide a robust security reference point for agencies that wish to transition their data and applications to a commercial cloud environment. The cloud security baseline articulated in this document incorporates cloud security analysis and recommendations that stem from the following four sources:

- Agency Use Cases: Some federal agencies are already leveraging commercial cloud environments, or are planning to make such transitions. A select few of these agencies have provided documentation of portions of their security architecture implementations. The known cloud security capabilities leveraged by these agencies in the cloud are included here as a part of the .gov cloud security baseline articulated in this document. The authors assume that the use case Agencies are leveraging security capabilities in addition to those in the available documentation, however these are unknown and are therefore not included in this document.
- Cloud Security Considerations: Similarly to traditional, on-premises networks, known and theorized malicious threats are present in commercial cloud environments. Certain characteristics of the commercial cloud environment, such as multitenancy, data distribution, and others, create new opportunities for malicious actors to access data in the cloud. Recommendations and guidance that address malicious threats in the commercial cloud and also address unique cloud risks are included as a part of the cloud security baseline articulated in this document.
- Cloud Community Recommendations: Cloud computing organizations, such as the Cloud Security Alliance, publish recommendations on cloud security best practices. For the purposes of this cloud security baseline for .gov, cloud computing publications were analyzed for any technical recommendations not already covered by the above baseline sources.

- .govCAR Guidance for Cloud Security: DHS continues to maintain and evolve its ability to defend Federal civilian agencies from threats in cyberspace. In support of this mission goal, the Network Security Deployment (NSD) division of the Office of Cybersecurity and Communications (CS&C), designs, develops, deploys, and maintains the National Cybersecurity Protection System (NCPS) and manages the Continuous Diagnostics and Mitigation (CDM) program. In support of these programs, NSD advances a variety of

technologies and other technical capabilities. NSD is leveraging a methodology called .govCAR, which is a cybersecurity capability investment portfolio prioritization tool. The .govCAR methodology maps current NSD capabilities against a suite of known cyber threats, aiming to identify areas where current capabilities are not fully addressing the cybersecurity need. As the .govCAR effort considers the commercial cloud environment, the resulting recommendations, affirmations, and observations will be incorporated into this cloud security baseline.

Assumptions

- All elements of the security baseline rely on documentation provided to DHS on current cloud architectures and security capability implementations and source information regarding cloud security. Where possible, elements of the security baseline reference existing literature and guidelines, such as those published by the National Institute of Standards and Technology (NIST).[1]
- The lists of baseline security elements that stem from Agency use cases should not be considered complete. The authors assume that these agencies leverage additional security capabilities in their cloud implementations beyond those provided in available documentation.
- No list of security guidance and capabilities is ever complete, in cloud environments or otherwise. As such, this baseline should not be considered a complete guide to securing data in a commercial cloud environment.
- Due to diversity across Agency missions and the types of data handled across .gov, each Agency should consider their unique security needs when transitioning to a commercial cloud.

Agency Cloud Use Cases

Federal agencies are already leveraging commercial cloud environments, or are currently in the process of planning such a transition. A select few of these agencies provided documentation regarding their planned cloud architecture implementations, including a subset of the security elements they plan to leverage. The known security capabilities leveraged by these agencies in the cloud are included as a part of the cloud security baseline articulated in this section.

Transitioning data and applications from a traditional, on-premises network to a commercial cloud environment can be a complex and challenging process. While, each Agency will develop its own cloud security plan to fit its individual data security needs within the specific cloud environment it plans to leverage, having an opportunity to observe how agencies have already implemented cloud security can be a helpful resource. Agencies that have already transitioned to the cloud may have incorporated lessons learned into their cloud security capability profile, and some may have gone through the process of working with their service provider to create security plans and protocols to handle a variety of security events.

[1] https://www.nist.gov/

It should be noted that the documentation made available by participating agencies varies, with no common format or purpose. As a result, the information and coverage of analyzed security capabilities in this part of the baseline may vary from use case to use case.

For each Agency use case, the available documentation was scoured for information and data on security-oriented capabilities leveraged to protect Agency data in the cloud. Once a security capability was identified, the security intent of that capability was abstracted to be included in the baseline. For example, if an Agency is leveraging a specific CAPTCHA function[2] in its cloud architecture, this security capability is captured in the cloud security baseline as "Verification of Human in the Loop". Multiple service providers provide verification of Human in the Loop capabilities, and an Agency can choose from any number of these providers if deemed appropriate for their individual data security needs. The intent of the baseline is to highlight the security capabilities leveraged by agencies currently, while remaining agnostic to the specific providers used by the agencies.

For each use case security capability, the way that the Agency has implemented the security element is discussed where possible. The purpose of the security feature is then discussed, and in addition, any additional guidance for agencies is provided.

Agency Use Case #1
Introduction:

In accordance with its mission, Agency #1 is planning to leverage a commercial cloud environment to support the data needs of a nation-wide survey. This survey will involve the collection of sensitive PII from surveyed individuals and the subsequent storage of this data in a commercial cloud environment for subsequent analysis by Agency employees. This Agency's configuration will include systems that support field infrastructure and internet data collection, including systems that will allow survey-takers to answer surveys online, which the Agency is depending on to enhance efficiency and to reduce costs.

Observations & Constraints:

- Agency #1 is currently leveraging the commercial cloud for its survey, however the survey will not take place for several years, and therefore any cloud cybersecurity lessons learned from this undertaking are not yet available. The currently available cloud security information is regarding the preparation for this Agency's cloud use and a complete picture of lessons learned from the use case will not be available until after survey activities are complete.
- Agency #1's survey effort is a substantial and unique undertaking that may not be substantially similar to most other government systems.

[2] http://captcha.net/

Diagram: Agency #1 high level cloud security architecture.

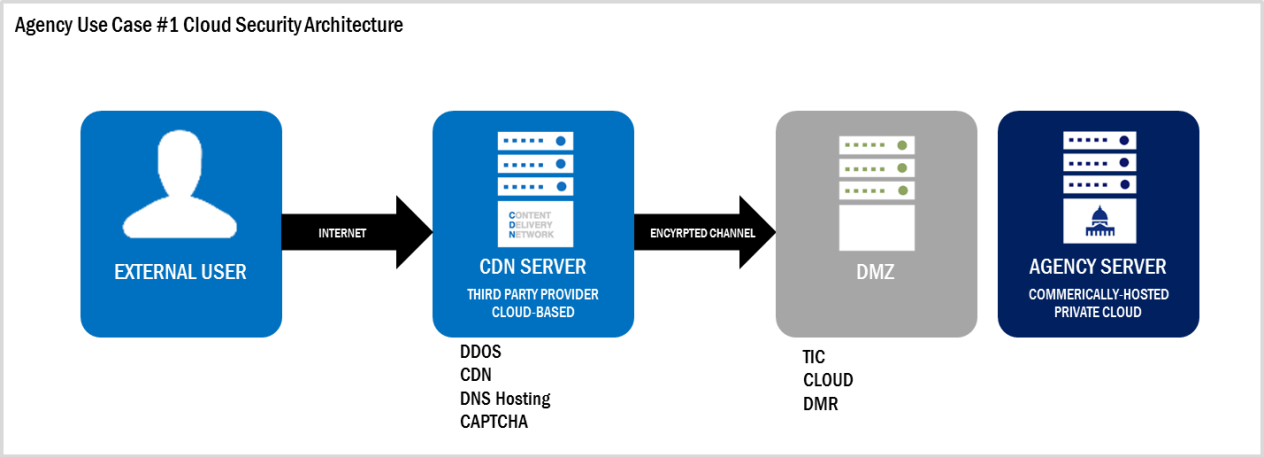


Diagram Description: Agency #1's configuration consists of a set of cloud server instances that will store survey data. In front of these server instances reside a set of virtual private clouds (VPCs) in series. A back end VPC consists of ingress and egress subnets. A second DMZ VPC represents a virtual perimeter that is intended to mimic a TIC environment. Finally, this Agency leverages a third party content delivery network (CDN) to handle identity management, DNS services, and general DDoS protection for online survey takers that access from the open internet.

Assumptions:

The baseline assumes that all of Agency #1's data is PII and is unclassified, and that the architecture does not include a SCIF and that there is no need for CSP personnel with security clearances. It is assumed that the connections between the general public and the DMZ are protected, presumably by TLS encryption, which enables the TIC to filter the traffic. The connections between the DMZ and the back end servers are also assumed to be protected, possibly by a VPN. The authors assume that the Agency #1 cloud architecture will have no incoming email, no outgoing email, and no outbound connections. The authors assume that encrypted traffic is inspected and analyzed. It should be noted that after the CDN provider approves a member of the general public to enter their survey data, the CDN provides that individual the address of a server on the TIC DMZ. Given knowledge of that address, an adversary could mount a DDoS attack directly, independent of the CDN.

Security Baseline Considerations:

This section will list each of the security capabilities implemented in the use case for Agency #1. It will discuss each capability, explain how it was implemented, explain the purpose of the capability, and provide additional guidance for security capability implementation that considers the uniqueness of the commercial cloud environment. This section will represent each capability at an abstract perspective to provide an understanding of how the capability can be applied in other situations to address similar issued.

Where possible, official cybersecurity policies are referenced for a given cybersecurity capability, such as FedRAMP.[3] The Federal Network Resilience (FNR) Trusted Internet Connections (TIC) Reference Architecture Document version 2.0 TIC Capability is explicitly referenced in cases where the Agency is leveraging a cloud security capability to address a TIC security technical requirement. When the Agency's implementation of a security capability was known, that implementation was indicated. In some cases, a security capability was known to have been addressed by the Agency, however its implementation was not known and therefore implementation information was not available for inclusion below.

1. **Network/Application/Host Security**
   a. **Intrusion Detection and Prevention Systems** (TS.INS.02)
      i. Implementation: The TIC access point passes all inbound/outbound network traffic through Network Intrusion Detection Systems (NIDS) configured with custom signatures, including signatures for the application layer. This includes, but is not limited to, critical signatures published by US-CERT.

      ii. Purpose: Intrusion Detection Systems are commonplace now and will be in place by most agencies as well as CSPs. Signatures by US-CERT is a more complicated situation due to licensing issues and the use of these will have to be agreed upon by both the Agency as well as the CSP.

   b. **Application Firewalls/Application Layer Filtering** (TS.CF.01) (FedRAMP SC-7, SC-7 (8))
      i. Implementation: The TIC access point uses a combination of application firewalls (stateful application protocol analysis), application-proxy gateways, and other available technical means to implement inbound and outbound application layer filtering. The TICAP will develop and implement a risk-based policy on filtering or proxying new protocols. Service providers are available to provide the appropriate tools to address this requirement.

      ii. Purpose: Application Layer Filtering addresses malicious and unauthorized actions, including bugs.

      iii. Additional Guidance: Application layer filtering goes beyond packet filtering and enables granular control on what enters or exits the network. While packet filtering can be used to completely disallow a particular type of traffic (for example, FTP), it cannot "pick and choose" between different FTP messages and determine the legitimacy of a particular FTP message. Application layer filtering, a more "intelligent" technology, can

[3] https://www.fedramp.gov/

do just that. Application layer filtering can be leveraged to look for abnormal information in the headers of a message and even within the data itself, and it can be set to look for specific character strings (words or phrases) within the message body and block messages based on that information. Thus, you can use Application layer filtering to prevent network attacks, or even to prevent internal users from sending particular sensitive information outside the network.

c. NCPS Participation (TS.INS.01) (FedRAMP AU-1, AU-6 (1), SC-7)

i. Implementation: The TIC access point participates in the National Cyber Protection System (NCPS). CSPs may consider this requirement to be a customer responsibility.

ii. Purpose: The purpose of this is to take advantage of Einstein capability, but CSPs don't have direct access to NCPS capabilities.

iii. Additional Guidance: This is an Agency responsibility and will have to be addressed by the Agency.

d. IPv6 (TM.TC.03) (FedRAMP CP-11)

i. Implementation: All TIC systems and components of the TIC access point support both IPv4 and IPv6 protocols in accordance with OMB Memorandum M-05-22 and Federal CIO memorandum "Transition to IPv6."

- The TICAP supports both IPv4 and IPv6 addresses and can transit both native IPv4 and native IPv6 traffic (i.e. dual-stack) between external connections and Agency internal networks. The TICAP may also support other IPv6 transit methods such as tunneling or translation.
- The TICAP ensures that TIC access point systems implement IPv6 capabilities (native, tunneling or translation), without compromising IPv4 capabilities or security. IPv6 security capabilities should achieve at least functional parity with IPv4 security capabilities.

ii. Purpose: The ability to handle IPv6 protocols anticipates planned changes in networking protocols without adversely affecting IPv4 capabilities.

e. Response Authority (TM.TC.05) (FedRAMP IR-8)

i. Implementation: The TICAP maintains normal delegations and devolution of authority to ensure essential incident response performance to a no-notice event. This includes, but is not limited to, terminating, limiting or modifying access to external connections, including to the Internet, based

on documented criteria, including when advised by US-CERT. Agencies can leverage available CSP access and flow control capabilities, including access control lists and security group features.

ii. Purpose: Allows TICAP to respond appropriately and in a timely manner to no-notice events and when advised by US-CERT.

f. TIC Staffing (TM.TC.06) (FedRAMP IR-1)

i. Implementation: The TIC management location, such as a Network Operations Center (NOC) and/or Security Operations Center (SOC), is staffed 24x7. On-scene personnel are qualified and authorized to initiate appropriate technical responses, including when external access is disrupted. CSPs should document network and security operations to include physical access and communications channels to communicate anomalies.

ii. Purpose: The appropriate staffing of TIC management locations enables proper incident response and limits potential negative impacts of events.

g. Denial of Service Response (TM.RES.03) (FedRAMP SC-5)

i. Implementation: The TICAP manages filters, excess capacity, bandwidth or other redundancy to limit the effects of information flooding types of denial of service attacks on the organization's internal networks and TICAP services. The TICAP has agreements with external network operators to reduce the susceptibility and respond to information-flooding types of denial of service attacks.

The Multi-Service TICAP mitigates the impact on non-targeted TICAP clients from a DOS attack on a particular TICAP client. This may include diverting information flooding types of denial of service attacks targeting a particular TICAP client in order to maintain service to other TICAP clients.

Agency #1 leverages a third party solution to mitigate DDoS attacks. (Please see security capabilities listed in the "User/Administrative User Authentication" section above for more detail).

ii. Purpose: This system is designed to address botnets from mounting DDoS attacks against the Agency's infrastructure. This capability is intended to prevent malicious traffic from reaching deeper parts of the Agency's IT infrastructure. Botnet protection also addresses credential fraud.

iii. Additional Guidance: Given the service that is being developed, there are considerations regarding what type of DDoS protection is needed. There are different classes of DDoS :

1. Network Layer Attacks : BGP network based attacks,
2. Application Layer Attacks: Having the ability to sort DDoS bots from regular human visitors. Here, bots can emulate humans and create high loads and interactions with the application, Solutions need to be immediately identified using a combination of signature-based and behavior-based heuristics.
3. DNS-Targeted Attacks

h. Web Session Filtering (TS.CF.02) (FedRAMP SC-7, SC-7 (8))

i. Implementation: The TIC access point filters outbound web sessions from TICAP clients based on, but not limited to: web content, active content, destination URL pattern, and IP address. Web filters have the capability of blocking malware, fake software updates, fake antivirus offers, phishing offers and botnets/key loggers calling home. Service providers are available to provide the appropriate tools to address this requirement.

ii. Purpose: Web Session Filtering addresses malicious and unauthorized actions from within network contacting addresses outside the network access point.

i. Encrypted Traffic Inspection (TS.CF.11)

i. Implementation: The TICAP has a documented procedure or plan that explains how it inspects and analyzes encrypted traffic. The document includes a description of defensive measures taken to protect TICAP clients from malicious content or unauthorized data exfiltration when traffic is encrypted. The TIC access point analyzes all encrypted traffic for suspicious patterns that might indicate malicious activity and logs at least the source, destination and size of the encrypted connections for further analysis.

ii. Purpose: Encrypted Traffic Inspection mitigates the potential for malicious or unauthorized exfiltration of data.

j. Secure all TIC Traffic (TS.PF.01) (FedRAMP AC-4, SC-7)

i. Implementation: All external connections are routed through a TIC access point, scanned and filtered by TIC systems and components according to

the TICAP's documented policy, which includes critical security policies when published by US-CERT. The definition of "external connection" is in accordance with the TIC Reference Architecture, Appendix A (Definition of External Connection).

ii. Purpose: The reason for this is to have standard security controls in one place so as to administer and update them in a standardized manner. In the Agency #1's implementation, this is most likely done via the TIC Cloud DMZ.

iii. Additional Guidance: This is an Agency responsibility and will have to be addressed by the Agency.

k. Default Deny (TS.PF.02)

i. Implementation: By default, the TIC access point blocks network protocols, ports and services. The TIC access point only allows necessary network protocols, ports or services with a documented mission requirement and approval.

ii. Purpose: The purpose is to limit the types of traffic that traverse this access point. This capability can be implemented by the CSP.

iii.

l. Stateless Filtering (TS.PF.03) (FedRAMP SC-7)

i. Implementation: The TIC access point implements stateless blocking of all inbound and outbound connections without being limited by connection state tables of TIC systems and components. Attributes inspected by stateless blocks include, but are not limited to:

Direction (inbound, outbound, interface)
- Source and destination IPv4/IPv6 addresses and network masks
- Network protocols (TCP, UDP, ICMP, etc.)
- Source and destination port numbers (TCP, UDP)
- Message codes (ICMP)

Agencies can leverage available CSP access control list capabilities to address this requirement.

ii. Purpose: A stateless firewall is one that maintains no connection state. If traffic is allowed in one direction but not the other, return traffic will be blocked. Section in Draft

m. Stateful Filtering (TS.PF.04) (SC-7)

i. Implementation: By default, the TIC access point blocks unsolicited inbound connections. For authorized outbound connections, the TIC access point implements stateful inspection that tracks the state of all outbound connections and blocks packets which deviate from standard protocol state transitions. Protocols supported by stateful inspection devices include, but are not limited to:

- ICMP (errors matched to original protocol header)
- TCP (using protocol state transitions)
- UDP (using timeouts)
- Other Internet protocols (using timeouts)
- Stateless network filtering attributes

Agencies can leverage available CSP security groups and/or third party providers to address this requirement.

ii. Purpose: A stateful firewall is one that maintains a connection's "state"- all traffic allowed in one direction, and will still allow for return entry of an established connection even if all other traffic is blocked.

n. Filter by Source Address (TS.PF.05)

i. Implementation: The TIC access point only permits outbound connections from previously defined TICAP clients using Egress Source Address Verification. It is recommended that inbound filtering rules block traffic from packet source addresses assigned to internal networks and special use addresses (IPv4-RFC5735, IPv6-RFC5156).

ii. Purpose: Source address validation verifies that a packet has been sent from a valid source address. This is accomplished by a routing table look-up by source address. The resulting interface should match the interface on which the packet has arrived and if not it will be dropped.

o. Asymmetric Routing (TS.PF.06) (FedRAMP AU-3 (1))

i. Implementation: The TIC access point stateful inspection devices correctly process traffic returning through asymmetric routes to a different TIC stateful inspection device; or documents how return traffic is always routed to the same TIC access point stateful inspection device.

ii. Additional Guidance: CSPs may have the ability to implement symmetric routing. It is recommended that Agencies work with their CSP to address this requirement if desired.

p. Botnet Protection

i. Implementation: Agency #1 uses a third party CDN for botnet protection. Requests to the Agency.gov URL are redirected to an ISR Authentication Static Landing Page, where the CDN Bot Manager evaluates the client browser. Browsers that successfully pass this evaluation are redirected to the Verification of Human in the Loop function.

ii. Purpose: This system is designed to address botnets from mounting DDoS attacks against the Agency's infrastructure. This capability is intended to prevent malicious traffic from reaching deeper parts of the Agency's IT infrastructure. Botnet protection also addresses credential fraud.

q. DNS Query Filtering – (TIC Capability TS.CF.13)

i. Implementation: TIC requirements state that the TIC access point system should filter DNS queries, and perform validation of DNS Security Extensions (DNSSEC) signed domains for TICAP clients. Agency #1 deploys a third party CDN DDoS Protection to address this requirement. In a traditional, non-cloud TIC system, the TICAP configures DNS resolving/recursive (also known as caching) name servers in accordance with, but not limited to, the following recommendations from NIST SP 800-81 Revision 1 (Draft):

1. The TICAP deploys separate recursive name servers from authoritative name servers to prevent cache poisoning.
2. The TICAP filters DNS queries for known malicious domains.
3. The TICAP logs at least the query, answer and client identifier.

It should be noted that Agency #1's CSP specifies that DNS filtering is a customer responsibility.

ii. Purpose: DNS Filtering mitigates malicious connections to a network. To eliminate the threat of forwarding DNS queries from unauthenticated hosts to unknown or untrusted servers (also known as domain-casting), DNS queries can be restricted from unauthenticated hosts to be forwarded explicitly to defined servers by defining DNS filters. Any DNS query from an unauthenticated host to a server not defined in a DNS filter are dropped.

2. User Authentication/Authorization

a. User/Administrative User Authentication – (TIC Capability TM.AU.01)

i. Implementation: User authentication is implemented to comply with NIST SP 800-53 identification and authentication controls for high impact systems (FIPS 199).[4] Administrative access to point devices requires multi-factor authentication (OMB M-11-11). Agency #1 uses an Identity Management System (IDMS) which is a collection of systems, processes, procedures, applications, database management systems, and interfaces that work together to perform the various functions of an integrated and automated IDMS. The IDMS provides services for the PIV Card request (if implemented), identity proofing, verification, background investigation and validation of an Applicant prior to PIV Card issuance. In its end state, the IDMS will include the following subsystem components:
    1. Authenticate accounts
    2. Set up external accounts

ii. Purpose: This system is designed to authenticate the identity of the user and to manage all account related information into an automated system. It also requires implementation of multi-factor authentication for privileged accounts and their subsequent maintenance.

iii. Additional Guidance: The authentication model when looking at IDMS on the cloud is significantly different at varying levels. As we move to the cloud, the attack surface changes from asset-centric security (endpoints – desktops, mobile devices, etc.) to an identity-centric approach. As such, every aspect of identity in the cloud must be considered and there are numerous architectural questions on how rights, privileges, and identity will be federated, retrieved, and stored. These considerations have impacts on both on-premises authentication, off premises Identity and Access Management (IdAM), and how trust is derived.

For instance, federation allows authenticating users from one security domain (such as their "home.gov", "sandia.gov", etc.) and authenticating them on another domain without the requirement for an intrinsic trust relationship between the two organizations. The organizations themselves may be running different operating systems (OS), directory services, certification authorities, and security protocols.

Federation is particularly important as services may run in unique and in varied security contexts. The services at the service delivery layer, the applications in the software layer, the virtual machines within the platform layer, the OS integral to the infrastructure layer, and the management consoles and services forming the management stack can then all use this

[4] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

federated environment for authentication, authorization, and role based access control.

b. Verification of Human in the Loop

i. Implementation: Agency #1 uses a CAPTCHA system in tandem with location-based identification for verifying that a human, rather than an automated entity, is attempting to interface with the Agency's system. Each survey-taker receives a code in the regular mail. When a survey-taker accesses the survey website, they are sent to a CAPTCHA provider, where they enter the code they received in the mail (along with the CAPTCHA) to verify that they are a human participant. Only human users who correctly enter both data entries are allowed to proceed to a CSP-hosted TIC DMZ VPC and fill out the survey.

ii. Purpose: This system is designed to verify that the user attempting to interface with the Agency's system is a human.

iii. Additional Guidance: Numerous tools can be used to incorporate these solutions. The captcha solutions are attempting to prevent bots submitting illegitimate content, malicious code insertion, among other issues. There are numerous considerations for captcha technologies, including delivery platforms (such as are these supported by mobile browsers), how much effort the service requires, external dependencies required by the service, the interact with web application firewalls, requirements for enabled active content, JavaScript requirements, reliance on browsers, and the user experience.

3. Data Protection

a. Reducing Cleartext (TS.CF.10) (FedRAMP IA-5)

i. Implementation: The TIC access point limits and documents the use of unauthenticated, clear text protocols for TIC management and will phase out such protocols or enable cryptographic authentication where technically and operationally feasible.

ii. Purpose: Reducing Cleartext improves the security of information transmission.

iii. Additional Guidance: There are numerous services such as reverse-proxies and layer 7 appliances that can be deployed at the boundary to transparently enforce encryption. There are questions on how certificates, encryption schemes (TLS vs SSL v3) that need to be considered.

4. Logging

a. Audit Storage Capacity (TIC Capability TM.DS.01) (FEDRAMP AU-4)

i. Implementation: Each TIC access point must be able to perform real-time header and content capture of all inbound and outbound traffic for administrative, legal, audit or other operational purposes. The TICAP has storage capacity to retain at least 24 hours of data generated at full TIC operating capacity. The TICAP is able to selectively filter and store a subset of inbound and outbound traffic.

Implementation of this requirement in the cloud could entail leveraging VPC Flow Logs to capture data flow metadata. These logs could be used with appropriate log retention for log aggregation. Agency #1's CSP, for example, could provide pertinent logs.

ii. Purpose: This system is designed capture network data as it traverses Agency #1's TIC Cloud DMZ and store it for 24 hours until it is filtered for long term storage of relevant data for future analysis

iii. Additional Guidance: Implementing a solution has several architectural considerations such as:

1. A layer 3 networking appliance such as an application firewall (such as F5 or Palo Alto Networks), network router, layer 2 firewall in order to intrude a device that can intercept the data.
2. Action on the data (such as filter, drop, redirect).
3. Providing the ability to mirror or save the data to a storage system.

b. Time Stamping (TM.LOG.02)

i. Implementation: All TIC access point event recording clocks are synchronized to within 3 seconds relative to Coordinated Universal Time (UTC). All TICAP log timestamps include the date and time, with at least to-the-second granularity. Log timestamps that do not use Coordinated Universal Time (UTC) include a clearly marked time zone designation. The intent is to facilitate incident analysis between TICAPs and TIC networks and devices.

CSPs should configure approved NTP providers within the customer environment to address this requirement.

ii. Purpose: Ensure accurate time stamping for TICAP events for future (incident) analysis.

iii. Additional Guidance: Considerations on geographically dispersed resources to ensure that time sync is effective and time zone information is

maintained for logs such that events from different resources are correlated for security relevant information.

c. Session Traceability (TM.LOG.03)

i. Implementation: The TICAP provides online access to at least 7 days of session traceability and audit ability by capturing and storing logs and files from installed TIC equipment including, but not limited to firewalls, routers, servers and other designated devices. The TICAP maintains the logs needed to establish an audit trail of administrator, user and transaction activity and sufficient to reconstruct security-relevant events occurring on, performed by and passing through TIC systems and components.

CSPs should provide traceability and auditability by providing logs with appropriate log retention policies in place.

ii. Purpose: Provide immediate online access to trace session connections and analyze security-relevant events. In addition, TM.LOG.04 requires retaining logs for an additional period of time either online or offline.

d. Log Retention (TM.LOG.04)

i. Implementation: The TICAP follows a documented procedure for log retention and disposal, including, but not limited to, administrative logs, session connection logs and application transaction logs. Record retention and disposal schedules are in accordance with the National Archives and Records Administration (NARA) Existing General Records Schedules, in particular Schedule 12, "Communications Records" and Schedule 20, "Electronic Records;" or NARA approved Agency-specific schedule. Note: This capability is intended for the management and operation of the TICAP itself, and does not require the TICAP infer or implement retention policies based on the content of TICAP client communications. The originator and recipient of communications through a TICAP remain responsible for their own retention and disposal policies.

CSPs should provide appropriate log retention and disposal policies.

ii. Purpose: Retain logs for an additional period of time either online or offline.

iii. Additional Guidance: One of the most significant challenges for an enterprise is sorting out how to run its operations from the cloud in order to perform proper log management. On a local network, logging is simple: an organization can point its devices to a local log management solution to

search and analyze log data. A local network has bandwidth for both standard traffic and log traffic. Log management is often equated to simple log aggregation, display, and storage—however this perspective does not take into account the complexity of log management. To address this challenge, considerations for other attributes such as event consolidation, correlation, limited real-time analysis, poor reporting and investigation flexibility, as well as integration of both identity and infrastructure context are recommended to be taken into account. Migration to a cloud environment raises additional question regarding this security capability. For example, how meaningful is the log data to be retained in the cloud? An Agency could leverage a private cloud to store and work with retained log data in an environment where they retain full access and control over it. Alternatively, an Agency could push retained logs to the commercial cloud service where they have limited access and limited control.

Logging in a public cloud is challenging. Visibility is severely reduced when system access and system/application controls are limited. Although cloud-based applications can boost productivity and availability of data, they are typically unable offer the same activity level that more traditional data-centers and public clouds can offer. Regardless of whether the model is IaaS or PaaS, there remain complications in keeping track of all the activity that occurs at different virtualized layers.

e. NTP Server (TM.LOG.01)

i. Implementation: Each TIC access point has a Network Time Protocol (NTP) Stratum 1 system as a stable Primary Reference Time Server (PRTS) synchronized within 0.25 seconds relative to Coordinated Universal Time (UTC). The primary synchronization method is an out-of-band NIST/USNO national reference time source (Stratum 0) such as the Global Positioning System (GPS) or WWV radio clock. See the TIC Reference Architecture, Appendix F for additional information.

CSPs have the ability to configure approved NTP providers within the customer environment to address this requirement.

ii. Purpose: Ensure accurate clock synchronization for the TIC access point.

5. Configuration Management

a. Asset Tracking – (TIC Capability TO.MG.01)

i. Implementation: The TIC requirement states that the system develops, documents, and maintains a current inventory of all TIC information systems and components, including relevant ownership information. Agency #1 deploys a web-based lifecycle asset management system designed to address local and global enterprise management needs for federal agencies.

b. Information System Recovery and Reconstitution (TIC Capability TM.DS.02) (FEDRAMP CP-2, CP-10)

i. Implementation: In the event of a TICAP system failure or compromise, the TICAP has the capability to restore operations to a previous clean state. Backups of configurations and data are maintained off-site in accordance with the TICAP continuity of operations plan.
Service provider operations personnel have 24x7 physical or remote accesses to management systems, which control the service devices. Using this access, operations personnel can terminate, troubleshoot or repair external connections, including to the Internet, as required.

Agency #1 could leverage CSPs capability of VM versioning, replication and life-cycle policies for backup. It could also leverage auto-scaling to recover from transient hardware failures.

ii. Purpose: System recovery

iii. Additional Guidance: Given the CSPs ability to conduct VM snapshotting and VM version control, many of the issues can be resolved natively though CSPs' current capabilities.

c. Least Functionality (TM.TC.02) (FedRAMP CM-7)

i. Implementation: TIC systems and components in the TIC access point are configured according to the principal of "least functionality," in that they provide only essential capabilities and specifically prohibit or restrict the use of non-essential functions, ports, protocols, and/or services.

6. Performance

a. Customer Service Metrics (TM.REP.01) (FedRAMP CA-7)

i. Implementation: The TICAP collects customer service metrics about the TIC access point, and reports them to its customers, DHS, and/or OMB as required. Examples of customer service metrics include, but are not limited to, performance within SLA provisions, issue identification, issue resolution, customer satisfaction, and quality of service.

ii. Purpose: Customer service metrics provide insight into performance and facilitate improvement.

b. Operational Metrics (TM.REP.02) (FedRAMP CA-7)

i. Implementation: The TICAP collects operational metrics about the TIC access point, and reports them to its customers, DHS, and/or OMB as requested. Examples of operational metrics include, but are not limited to, performance within SLA provisions, network activity data (including normal and peak usage), and improvement to customer security posture.

ii. Purpose: Operational service metrics provide insight into performance and facilitate improvement.

Agency Use Case #2

Introduction:

In accordance with its mission, Agency #2 handles a significant quantity of data that is used by researchers both internal and external to the Agency. Agency #2 would like to integrate more cloud resources to facilitate greater data availability to its external researchers, and to enhance the ease of ingesting data from its external data sources. The observations and analysis included here are drawn from a cloud implementation guide drafted by Agency #2. The guide does not mention any specific cloud providers or cloud services by name. However, the document is meant to highlight network security patterns for implementing general cloud-based services from this Agency. The document heavily references the TIC Reference Architecture 2.0 and FedRAMP programs in the description of the security patterns, and therefore the security capabilities listed by Agency #2 are often described as pursuant to TIC security capability requirements. Therefore, it should be noted that the list of security considerations included here should not be considered to be the complete list of security capabilities leveraged by this particular Agency. It is likely that only the considerations relating to TIC requirements are included in this use case, and that this Agency leverages additional security capabilities in its commercial cloud implementation that are unknown.

The Agency #2 cloud implementation guide organizes its cloud security architecture into security patterns. These patterns are described below and are referenced throughout this Agency's use case security capabilities list.

Observations & Constraints:

- The Agency #2 use case is written in a very general manner, due to the lack of knowledge of the specific cybersecurity approaches this Agency intends to implement.

Diagrams: The overview cloud security architecture figure and security pattern figures for Agency use case #2.

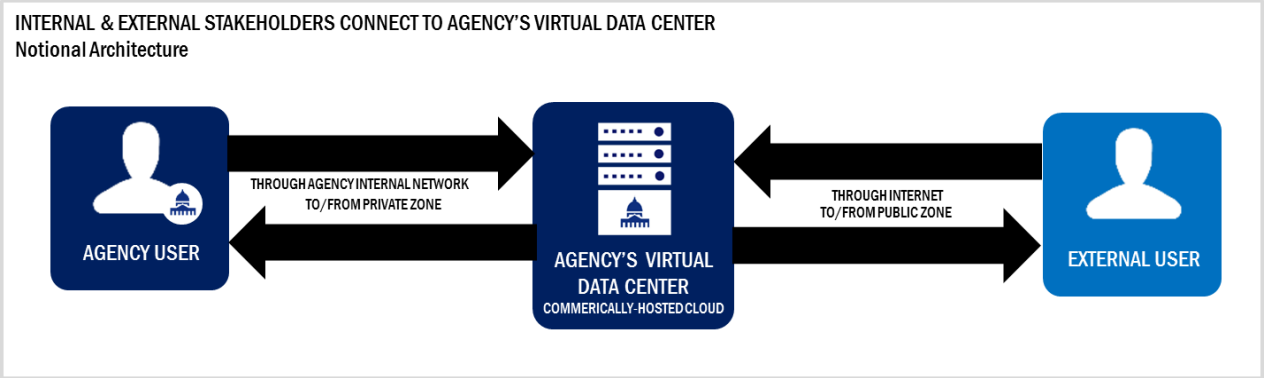


Figure 1: Agency Use Case #2 Overview Graphic

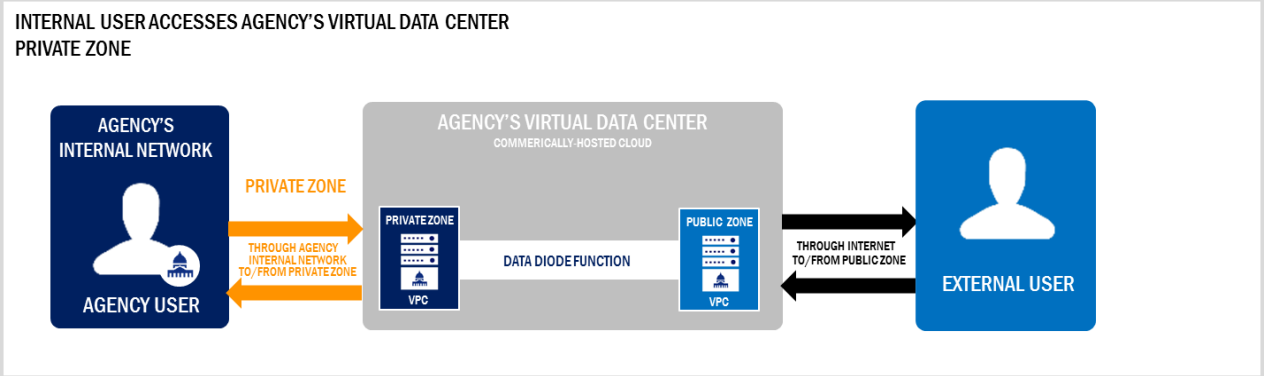


Figure 2: Private Zone

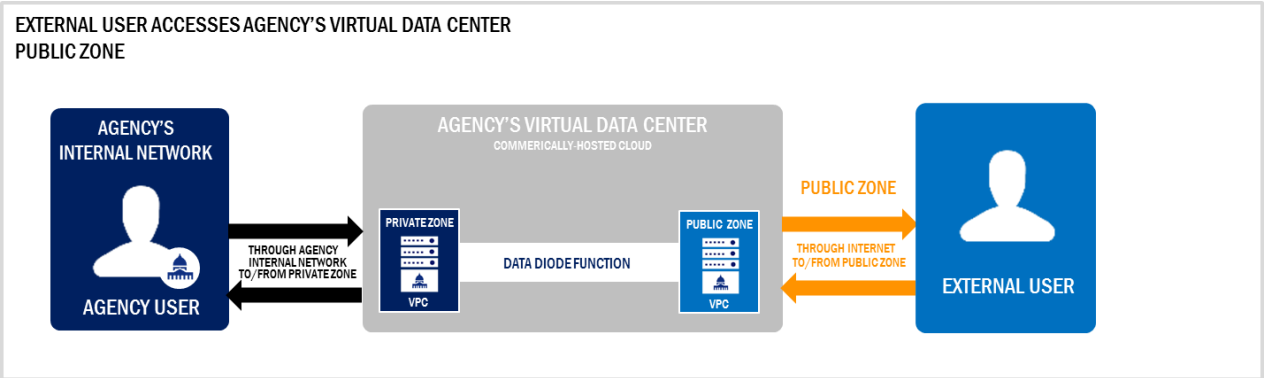


Figure 3: Public Zone

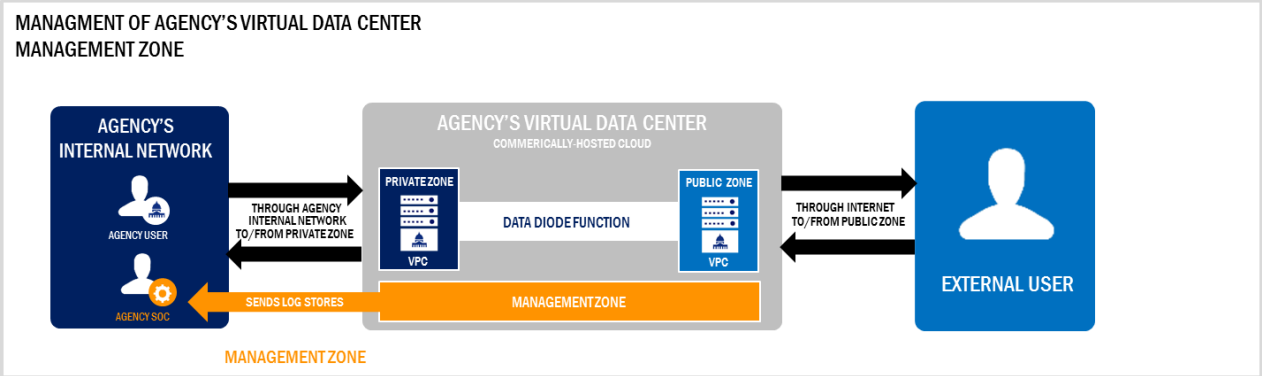


Figure 4: Management Zone

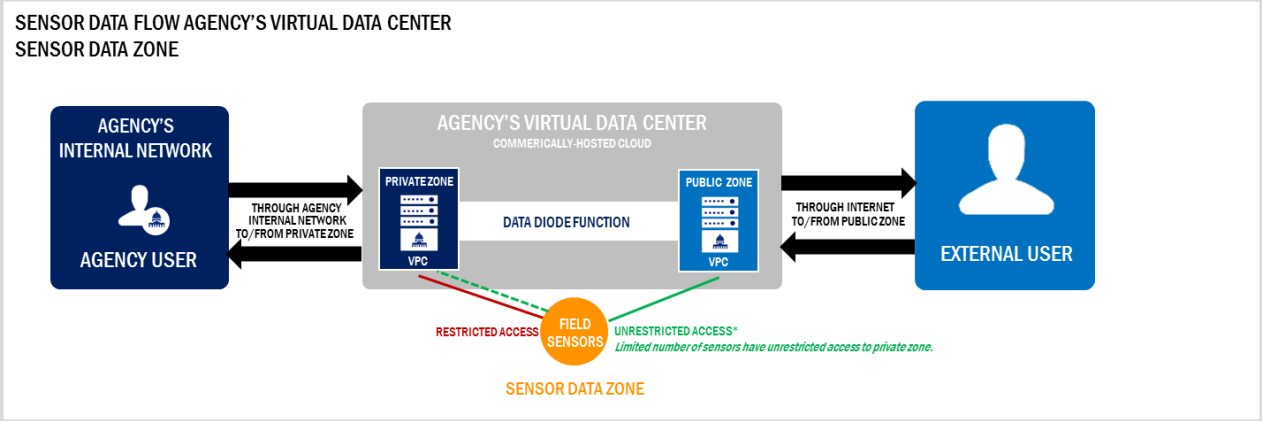


Figure 5: Sensor Data

Description: The Agency #2 use case is divided into security patterns (Figures 1-4):

1. Agency Use Case #2 overview graphic representing the high level cloud security architecture.
2. The "private zone": a virtual data center, hosted on a cloud provider that is only accessible by authorized Agency users from the Agency network.
3. The "public zone": a virtual data center, hosted on a cloud provider that is publicly accessible from the Internet. This zone can only contain data that with unrestricted access. There is a data diode function that can be used to transfer unrestricted access data from the private zone into the public zone.
4. The "management zone": a virtual data center, hosted on a cloud provider that is only accessible by authorized Agency users from the Agency network. This data center is used for administering services in both the public and private zones, and as such has administrative access to components in both types of zones.
5. Sensor data: Data may be provided by remote sensors directly into both the public and private zones. This data may either be "unrestricted", meaning that it is immediately

available for public consumption and may be ingested into the public or private zones, or "restricted" meaning that it must first be validated or combined with other data before it is made available for public consumption, and can only be ingested into the private zone.

Assumptions: Section in Draft

Security Baseline Considerations:

This section will list each of the cloud security capabilities implemented in the use case for Agency #2. It will discuss each capability, explain how it was implemented if known, explain the purpose of the capability, and provide additional guidance for capability implementation. This section will represent each capability at an abstract perspective to provide an understanding of how the capability can be applied in other situations to address similar issued.

Where possible, the FNR TIC Reference Architecture Document version 2.0 TIC Capability is explicitly referenced in cases where the Agency is leveraging a cloud security capability to address a TIC security technical requirement.

1. **Network/Application/Host Security**
    a. **Network Isolation** – (TIC Capabilities TS.PF.01, TS.PF.02, TS.PF.03, TS.PF.04, TS.CF.01)
        i. Implementation: The "public zone", "private zone" and "management zone" services and components will be protected from arbitrary connections from the Internet. The "private zone" will only be accessible from the Agency #2 Agency network, or the "management zone". Services in each zone will only be made available with a documented use case, and proper routing through appropriate security devices. The "public zone", "private zone" and "management zone" will not access external resources (e.g. the Internet) without a documented use case (e.g. ingesting sensor data, updating anti-virus, etc.). This "network isolation" will form a key part of the "data diode", ensuring that the "public" zone cannot retrieve data from the "private" zone, and that only authorized data from the "private" zone can be pushed into the "public" zone. Exact isolation implementation details are not known, however Agency #2 will likely use a combination of firewalls, access control lists, and cloud configurations to enforce this isolation.

        ii. Purpose: To minimize the opportunities for external attacks on the zones as well as to decrease the channels available for C2 or exfiltration.

        iii. Additional Guidance: The relevant TIC guidance:
        "By default, the TIC access point blocks network protocols, ports and services. The TIC access point only allows necessary network protocols, ports or services with a documented mission requirement and approval."

"The TIC access point implements stateless blocking of all inbound and outbound connections without being limited by connection state tables of TIC systems and components. Attributes inspected by stateless blocks include, but are not limited to:

Direction (inbound, outbound, interface)
- Source and destination IPv4/IPv6 addresses and network masks
- Network protocols (TCP, UDP, ICMP, etc.)
- Source and destination port numbers (TCP, UDP)
- Message codes (ICMP)

"By default, the TIC access point blocks unsolicited inbound connections. For authorized outbound connections, the TIC access point implements stateful inspection that tracks the state of all outbound connections and blocks packets which deviate from standard protocol state transitions. Protocols supported by stateful inspection devices include, but are not limited to:

- ICMP (errors matched to original protocol header)
- TCP (using protocol state transitions)
- UDP (using timeouts)
- Other Internet protocols (using timeouts)
- Stateless network filtering attributes"

"The TIC access point uses a combination of application firewalls (stateful application protocol analysis), application-proxy gateways, and other available technical means to implement inbound and outbound application layer filtering. The TICAP will develop and implement a risk-based policy on filtering or proxying new protocols."

b. Intrusion Detection and Prevention Systems – (TIC Capability TS.INS.02)

i. Implementation: The "public zones" and "private zones" will contain a variety of attack surfaces and the Agency will make use of cloud-native Intrusion Detection and Prevent Systems (IDPS) to detect and mitigate attacks.

ii. Purpose: To detect and prevent attacks on the zones from both the Internet as well as from the Agency network.

iii. Additional Guidance: To comply with TS.INS.02, the signatures used with this IDPS must include, but are not limited to, critical signatures published by US-CERT.

c. **Application Firewalls/Application Layer Filtering** – (TIC Capabilities TS.CF.01, TS.CF.03)
   i. Implementation: The "public zones" and "private zones" will contain a variety of web applications and may include other non-web applications. These applications may be accessed by both authenticated and authorized, untrusted users, as well as, for applications in the public zone, unauthenticated users. These applications will only be made available through Web Application Firewalls. The Agency will be deploying cloud-native Web Application Firewalls for services in the public zone, as well as a Web Application Firewall for services in the private zone that may either be hosted in the Agency or in the CSP.

   ii. Purpose: To mitigate application attacks on the zones from both the Internet as well as from the Agency network.

   iii. Additional Guidance: (Section in Draft)

d. **NCPS Participation** – (TIC Capabilities TS.INS.01)
   i. Implementation: Agency #2 will configure all external traffic to or from the "management" and "private" zones to be routed through their enterprise network, through their Agency TIC, which participates in NCPS, and to the external resource. DNS configuration for the "management" zone will be configured to use the Agency DNS server, enabling participation in E^3A.

   ii. Purpose: To ensure NCPS protections are available for sensitive data, and for situational awareness to NCICC.

   iii. Additional Guidance: External traffic to and from the public zone will not be configured to pass through NCPS protections. Some combination of the service logs, IDPS logs and firewall logs should be provided to NCPS to provide them situational awareness to address this gap.

2. **User Authentication/Authorization**
   a. **User/Administrative User Authentication** – (TIC Capability TM.AU.01)
      i. Implementation: To comply with NIST SP 800-53 identification and authentication controls for high impact systems (FIPS 199). Administrative access to point devices requires multi-factor authentication (OMB M-11-11). Agency #2 uses an Identity Management System (IDMS) which is a collection of systems, processes, procedures, applications, database management systems, and interfaces that work together to perform the various functions of an integrated and automated

IDMS. The IDMS provides services for the PIV Card request (if implemented), identity proofing, verification, background investigation and validation of an Applicant prior to PIV Card issuance. Each zone will have its own IDMS databases so that accounts cannot be shared across zones, decreasing opportunities for lateral movement from one zone to another.

ii. Purpose: This system is designed to authenticate the identity of the user and to manage all account related information into an automated system. It also requires implementation of multi-factor authentication for privileged accounts and their subsequent maintenance.

iii. Additional Guidance: (Section in Draft)

b. Authorization

i. Implementation: Agency #2 plans to use a Role-Based Access Control mechanism for authorizing access to services in the "public", "private" and "management" zones. These mechanisms will be used to ensure a "least privilege" approach to access to services and components inside each zone. They will be used to control levels of access to the services, their configuration, and to data contained within the services.

ii. Purpose: To ensure that only individuals with appropriate access to services or data are able to access it.

iii. Additional Guidance: (Section in Draft)

c. Remote Management Access

i. Implementation: Agency #2 will use either a private connection to the cloud, an IPsec tunnel or other encrypted means of connecting their Agency network with the "management" zones. The "management" zone can then be used to manage the other two zones. The accounts in this zone will differ from those in the Agency network, and in the other zones to avoid lateral movement from a zone into the "management zone.

ii. Purpose: To provide the Agency with secure access to manage all the zones.

iii. Additional Guidance: (Section in Draft)

3. Data Protection

a. Encryption in Transit

i. Implementation: Agency #2 will have two methods of ingesting data into their data centers: data pushed from the Agency, and data from remote sensors. The connections for data pushed from the Agency will be encrypted by either VPN, TLS, IPsec or other encrypted method. The connections for data from the sensors will be encrypted with TLS.

ii. Purpose: To ensure that data cannot be accessed by eavesdroppers listening to network communications with the zones.

iii. Additional Guidance: (Section in Draft)

b. Encryption at Rest

i. Implementation: Agency #2 will encrypt all restricted data in the private zones.

ii. Purpose: To mitigate the opportunities for data to be retrieved by individuals with access to the storage location of the data.

iii. Additional Guidance: Additional guidance for encrypting data can be found in FIPS 197, 199, and 200.

c. Key Management

i. Implementation: Agency #2 will have numerous encryption keys to handle various encryption needs, including but not limited to, certificates for the services, and encryption keys for data at rest and in transit.

ii. Purpose: To centralize and protect the encryption keys needed to access the services and protect restricted data.

iii. Additional Guidance: (Section in Draft)

4. Logging

a. **Audit Storage Capacity** (TIC Capability TM.DS.01) (FEDRAMP AU-4)

i. Implementation: (Section in Draft)

ii. Purpose: (Section in Draft)

iii. Additional Guidance: Implementing a solution has several architectural considerations such as:

1. A layer 3 networking appliance such as an application firewall (such as F5 or Palo Alto Networks), network router, layer 2 firewall in order to intrude a device that can intercept the data
2. Action on the data (such as filter, drop, redirect)
3. Providing the ability to mirror or save the data to a storage system.

b. **Time Stamping -** (TIC Capabilities TM.LOG.01, TM.LOG.02)
   i. Implementation: All TIC access point event recording clocks are synchronized to within 3 seconds relative to Coordinated Universal Time (UTC). All TICAP log timestamps include the date and time, with at least to-the-second granularity. Log timestamps that do not use Coordinated Universal Time (UTC) include a clearly marked time zone designation. The intent is to facilitate incident analysis between TICAPs and TIC networks and devices.

      As with NTP (network time protocol) Server, CSP will "configure approved NTP providers within the customer environment." [5]

   ii. Purpose: Ensure accurate time stamping for TICAP events for incident analysis.

   iii. Additional Guidance: Considerations on geographically dispersed resources to ensure that time sync is effective and time zone information is maintained for logs such that events from different resources can be correlated for security relevant information.

c. **Session Traceability** (TIC Capability TM.LOG.03)
   i. Implementation: The TICAP provides online access to at least 7 days of session traceability and audit ability by capturing and storing logs / files from installed TIC equipment including, but not limited to firewalls, routers, servers and other designated devices. The TICAP maintains the logs needed to establish an audit trail of administrator, user and transaction activity and sufficient to reconstruct security-relevant events occurring on, performed by and passing through TIC systems and components.

      Agency #2 will aggregate logs from the public and private zones on the management zone, for access to their SOC, and to provide a subset of log information to the SOC.

   ii. Purpose: provide immediate online access to trace session connections and analyze security-relevant events. In addition, TM.LOG.04 requires retaining logs for an additional period of time either online or offline.

   iii. Additional Guidance: (Section in Draft)

d. **Log Retention** (TIC Capability TM.LOG.04)

[5] Ibid.

i. Implementation: The TICAP follows a documented procedure for log retention and disposal, including, but not limited to, administrative logs, session connection logs and application transaction logs. Record retention and disposal schedules are in accordance with the National Archives and Records Administration Existing General Records Schedules, in particular Schedule 12, "Communications Records" and Schedule 20, "Electronic Records;" or NARA approved Agency-specific schedule. Note: This capability is intended for the management and operation of the TICAP itself and does not require the TICAP infer or implement retention policies based on the content of TICAP client communications. The originator and recipient of communications through a TICAP remain responsible for their own retention and disposal policies.

Agency #2 will aggregate logs from the public and private zones on the management zone, for access for their SOC, and to provide a subset of log information to the SOC.

ii. Purpose: Retain logs for an additional period of time either online or offline.

iii. Additional Guidance: (Section in Draft)

5. Configuration Management

a. **Asset Tracking** – (TIC Capability TO.MG.01)

i. Implementation: The TIC requirement states that the system develops, documents, and maintains a current inventory of all TIC information systems and components, including relevant ownership information.

Agency #2 will likely include a method to automatically scale service resources to meet demand. As these scaling procedures will be automatic, robust logging of changes to resource available will need to be included, and the specifics of the resource elasticity will be managed through appropriate DevOps procedures to ensure the possibilities for system asset expansion well documented.

ii. Purpose: System awareness and recovery.

iii. Additional Guidance: (Section in Draft)

b. **Configuration Management** – (TIC Capability TO.MG.02)

i. Implementation: The TIC requirement states that the system follows a formal configuration management and change management process to maintain a proper baseline.

Agency #2 will leverage appropriate DevOps procedures to ensure that all changes to the services and components in the zones are stored in a version control system.

ii. Purpose: System recovery

iii. Additional Guidance: (Section in Draft)

c. Information System Recovery and Reconstitution - (TIC Capability TM.DS.02) (FEDRAMP CP-2, CP-10)

i. Implementation: In the event of a TICAP system failure or compromise, the TICAP has the capability to restore operations to a previous clean state. Backups of configurations and data are maintained off-site in accordance with the TICAP continuity of operations plan.

Service provider operations personnel have 24x7 physical or remote access to management systems, which control the service devices. Using this access, operations personnel can terminate, troubleshoot or repair external connections, including to the Internet, as required.

Agency #2 will leverage appropriate DevOps procedures, and cloud native life-cycle policies for backup. It should also leverage auto-scaling to recover from transient hardware failures.

ii. Purpose: System recovery

iii. Additional Guidance: Given the CSPs ability to conduct VM snapshotting and VM version control, many of these issues can be resolved natively though CSPs' current capabilities.

d. System Elasticity - (TIC Capability TM.DS.02) (FEDRAMP CP-2, CP-10)

i. Implementation: Agency #2 will likely include a method to automatically scale service resources to meet demand. As this will be designed to be automatic, robust logging of changes to resource available will be included, and the specifics of the resource elasticity will be managed through the DevOps procedures.

ii. Purpose: (Section in Draft)

iii. Additional Guidance: Given the CSPs ability to conduct VM snapshotting and VM version control, many of the issues can be resolved natively though CSPs' current capabilities.

6. **Performance**
   a. **Content Distribution Network**
      i. Implementation: Agency #2 will employ a Content Distribution Network for unrestricted data in the "public" zone. It may also be used for restricted access data in the "private" zone with a FIPS 199 category of Low or Moderate.

      ii. Purpose: To allow for high availability, high performance access to data.

      iii. Additional Guidance: (Section in Draft)

   b. **Load Balancer**
      i. Implementation: Agency #2 will employ load balancers to provide the ability to expand services to meet the required demand.

      ii. Purpose: To allow for high availability, high performance access to data.

      iii. Additional Guidance: (Section in Draft)

Agency Use Case #3

Introduction:

Agency #3 implements a defense in depth approach and what also appears to be overlapping tool sets to ensure a high degree of situational awareness and defense. Agency #3 plans to use multiple cloud services providers to fulfill its data, application, and email needs. To provide an optimal user experience, the Agency utilizes multiple zones for redundancy along with load balancers, SSL offloading and other components. The Agency plans to do role based segregation of traffic and leverage multiple inspection points to monitor network traffic. To accompany this security model, the Agency plans to monitor and to analyze numerous types of logs, network, server, application, endpoint, authentication, etc. for anomalous behavior and for emerging threats.

Agency #3 leverages what they refer to as a "hybrid" cloud approach. For Use Case #3, hybrid means that the Agency is leveraging private cloud space with one CSP, while leveraging public cloud space at two additional CSPs for other services.

Observations & Constraints:

- The Agency uses a hybrid cloud approach that directly connects data in their private cloud with data and services in their public cloud.
- The Agency uses a number of security services that seem to overlap or offer redundant capabilities.
- The Agency utilizes a defense-in-depth approach including micro-segmentation.

Diagram: (Section in Draft)

Diagram Description: (Section in Draft)

Security Baseline Considerations:

This section will list each of the security capabilities implemented in the use case for Agency #1. It will discuss each capability, explain how it was implemented, explain the purpose of the capability, and provide additional guidance for security capability implementation that considers the uniqueness of the commercial cloud environment. This section will represent each capability at an abstract perspective to provide an understanding of how the capability can be applied in other situations to address similar issued.

When the Agency's implementation of a security capability was known, that implementation was indicated. In some cases, a security capability was known to have been addressed by the Agency, however its implementation was not known and therefore implementation information was not available for inclusion below.

1. **Network/Application/Host Security**
    a. **Network Isolation –** Virtual local area networks (VLANs)
        i. Implementation: Agency #3 will deploy a Hybrid Cloud network environment solution using virtual private clouds (VPCs) and Software Defined Networking, such as VLANS, that perform role-based traffic segregation (e.g., management, development, etc.) and each is governed by network policy enforcement points and packet filtering.

        ii. Purpose: Segregation of traffic based on functionality (e.g. management, development, etc.) to enable enforcing policies on specific traffic flows and to provide ease of network traffic monitoring. Different policies can apply to a specific type of traffic. Traffic segregation enables policy enforcement based on traffic type and functionality. When networks have similar traffic they are (in theory) easier to monitor because the traffic is expected to be similar vis-à-vis observing monitoring disparate traffic on the network while also looking for anomalies.

        iii. Additional Guidance: If desired by an Agency, traffic isolation approaches can be quite granular and can be based on traffic type, its destination, and port number, among other isolation approaches if desired. Some CSPs

provide "Next Generation" firewalls that Agencies can purchase. Next Generation firewalls are still firewalls, and it is recommended that Agencies examine the additional security functionality of any Next Generation capability to determine if it is needed to meet their security needs before purchasing.

b. Intrusion Detection and Prevention Systems

iii. Implementation: Agency #3 accomplishes IDS/IPS by leveraging a commercial inline IPS product for all inbound and outbound traffic, regardless of traffic origination and destination. After traversing the IPS the traffic is inspected by the commercial firewalls and then again by additional IPS devices before it is passed to the private cloud datacenter LANs or to public cloud VPCs (please see Agency Use Case #3 introduction for more detail on this hybrid cloud architecture). This IPS approach is also applied to inbound and outbound traffic directly passing between the Agency's private and public cloud environments that bypasses an ISP.

iv. Purpose: To detect threats to the integrity of the network and remediate them.

c. Traffic Anomalies and Emerging Threat Detection

i. Implementation: Agency #3 leverages multiple security devices capable of detecting traffic anomalies and threat detection such products from a variety of third party vendors.

ii. Purpose: To identify and protect networks from emerging threats where current known IDS and IPS signatures are inadequate.

d. Encrypted Traffic Analysis

i. Implementation: Agency #3 plans to perform analysis on all encrypted both entering and leaving their networks by using a third party vendor SSL decryption capabilities.

ii. Purpose: To gain visibility into all traffic on the network, rather than only have visibility into unencrypted traffic.

e. Packet Filtering

i. Implementation: Agency #3 plans to perform packet filtering on all packets going into and out of their VPCs and in and out of their network using a third party commercial service.

ii. Purpose: To inspect traffic at the packet level for increased security**.**

f. Endpoint Security and Policy-Based Enforcement

i. Implementation: Agency #3 accomplishes endpoint security and policy-based enforcement through commercial providers that support CDM Phase 1 endpoint and policy-based security services. These capabilities can identify numerous vulnerabilities such as outdated antivirus and malware signatures, endpoints not running security software such as antivirus and malware software, open ports that should be closed on endpoints, and old or unpatched versions of software on endpoints. These capabilities can also identify what certificates exist on endpoints, along with what OS and OS version endpoints are running.

ii. Purpose: To ensure endpoints meet a minimum security threshold and that potential vulnerabilities are identified so security personnel can address potential issues appropriately and promptly.

g. Systems Management

i. Implementation: Agency #3 will use a variety of commercial 3rd party system management security tools for systems management. Additionally, commercial data analysis tools will be leveraged to help detect changes to cloud resources, configuration and system settings. Agency #3 plans to base images from a gold standard image.

ii. Purpose: To ensure systems are authorized and accounted for, have baseline security policies applied and are in compliance with the policies, and are monitored for activity and health.

h. Vulnerability Scanning

i. Implementation: Multiple commercial third party vulnerability scanning tools will be leveraged by Agency #3 to scan for vulnerabilities and to perform vulnerability analysis. Vulnerabilities can be software, networking, or OS-based.

ii. Purpose: To identify and to detect nodes with vulnerabilities or potential vulnerabilities so that security personnel can evaluate any issues and provide remediation if necessary.

1. User Authentication/Authorization

a. User/Administrative User Authentication

i. Implementation: Agency #3 accomplishes user and administrative user authentication with a collaboration of approaches. Agency #3 leverages a commercially available directory service in conjunction with the Terminal

Access Controller Access Control System Protocol (TACACS) and another commercially available identity and access management service. Additional user authentication protections will be implemented including password policies requiring passwords be changed after a designated time period. Agency #3 will also provide monitoring and enforcement of authentication policies by using their commercial directory service and CDM Phase 1, 2, & 3 capabilities.

ii. Purpose: This system is designed to authenticate the identity of the user and to manage all account related information into an automated system.

iii. Additional Guidance: TACACS is an older technology and has been replaced by TACACS+. From available use case documentation, the authors are assuming that Agency #3 will be leveraging the more recent protocol due to its stronger security compared to TACACS. Use case detail was not available regarding how the commercial directory service will be implemented in the cloud, for example whether it will be its own unique set of credentials or will be synchronized with an LDAP (lightweight directory access protocol) provider. Agency #3 use case documentation states that there will be physical access controls systems in place, but no specifics regarding this were found in the documentation, and generally in a cloud environment the tenant does not have control over physical security access.

b. Multi-Factor Authentication (MFA)

i. Implementation: Agency #3 plans to leverage MFA by implementing HSPD-12 (CAC) cards and with the use of RSA's SecurID.

ii. Purpose: To provide an additional authentication verification of a user, in this case adding something a user has (CAC card or SecurID card) to augment something a user knows (password or pin for the CAC card or SecurID card)

c. Authorization

i. Implementation: Agency #3 authorization is accomplished through a commercial third party directory service via their TACACS implementation. Agency #3 states that this service will log and monitor users actions. Authorization access policy monitoring and enforcement will be accomplished via the directory service in conjunction with DHS CDM Phase 1, 2, 3 and HSPD-12 implementations.

ii. Purpose: To ensure that users or service accounts can only access the resources that they are explicitly allowed to access and to ensure accounts can only perform actions on resources in accordance to the account's specified privileges.

iii. Additional Guidance: Agency #3 does not explicitly state how authorization will be executed. One possibility is that identity and access management roles will be mapped to the Agency's directory service. Each Agency's data center user role implementation will vary by individual Agency need.

d. Login Analysis

i. Implementation: Agency #3 will use CDM to monitor and analyze login events.

ii. Purpose: To identify logins that are usual such as a user actively logged in with IP addresses from different geoIP regions, or to identify accounts that may be compromised or attempting to be compromised.

iii. Additional Guidance: Login events can occur within multiple areas within the cloud architecture, and therefore it is critical that all logs capturing login attempts are identified and evaluated for monitoring.

e. Remote Access Control

i. Implementation: In-band remote access connections are secured via encrypted network dynamic multipoint virtual private networks (DMVPNs), encrypted host-based VPNs, and SSL-based web connectivity supported by Agency #3's two-factor authentication and network access policy enforcement controls. Out-of-band network connectivity is secured by administrative users from restricted IP address allocations (IP whitelisting) using a commercial third party VPN service, TACACS authentication, and SSL-based connectivity. All SSL connections are secured by Agency #3 certificates. According to the documentation provided, all GFE users accessing resources remotely via MTIPS will be required to use the Agency's PulseSecure VPN implementation.

ii. Purpose: To secure all remote access connections.

3. Data Protection

a. Data Encryption - Transit

i. Implementation: Agency #3 accomplishes data encryption by the MPLS edge routers and the Mission DMVPNs. These connections and all other

secured devices will adhere to NIST 800-57 standards and leverage FIPS 140-2 compliant signed certificates, algorithms and cipher, which include using the Agencies PKI policies and certificates. Additionally, AES-256 encryption will be used.

ii. Purpose: Encryption is enabled throughout the network to ensure data privacy.

b. Data Encryption – Data at Rest

i. Implementation: Use case #3 documentation states that security features on the private cloud include encryption at rest capabilities along with instantaneous enabling and disabling of encryption. No additional implementation details are provided. On the public cloud, Agency #3 plans to leverage encryption, but as with the private cloud few details are provided.

ii. Purpose: To protect the confidentiality of data at rest (on storage devices)

iii. Additional Guidance: With few details on encryption at rest, it would be ideal to see more information on protecting data on both the private and public cloud storage along with more details on encryption key management.

c. Unauthorized Storage Usage Protection and Monitoring

i. Implementation: This security capability is accomplished via the security controls and logging that consists of syslog and several commercially available third parts cloud logging facilities.

Agency #3 private cloud storage security includes:

1. Instantaneous enable/disable encryption
2. Encrypt data at rest at a cluster-wide level
3. Instantaneously and securely sanitizing data
4. Rotating passwords per security policy intervals
5. Ability to enable/disable on-disk encryption with live data using an Agency-assigned key
6. Ability to transform the cluster from a secure configuration to non-secure configuration (and vice-versa)
7. Securely sanitize a specific partition and subsequently use it for storing data from other partitions that are being marked un-secure

ii. Purpose: To protect and monitor against unauthorized storage usage.

d. Unauthorized Storage Access Protection and Monitoring

i. Implementation: Agency #3 accomplishes unauthorized storage access protection and monitoring via the security controls and logging that consists of syslog, CSP-provided logging facilities.

ii. Purpose: To ensure only the appropriately authorized users or services can access data.

iii. Additional Guidance: Use case #3 documentation did not provide specific details regarding implementation of this security capability. To provide adequate guidance to Agencies details, ideally details for each cloud type would be made available, since both a private and a public cloud are being leveraged by Agency #3.

e. Key Management

i. Implementation: Agency #3 hybrid cloud devices and hosts are equipped with security capabilities that may use the Agency's NIST compliant PKI implementation. Any private or public cloud host or device will be deployed following the Agency's PKI policies. If the Agency's PKI implementation is unavailable to a device or host, a self-signed certificate will be temporarily used.

ii. Purpose: Organizations leverage public key infrastructure (PKI) to establish a set of roles, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and to manage public-key encryption.

iii. Additional Guidance: Remove all certificate authorities from browsers where the certificate authority may be questionable. Also, if a self-signed certificate temporarily used, it's important that appropriate personnel are aware of the self-signed certificate and that it be resolved within a defined time period.

f. Secure Erase

i. Implementation: The Agency has stated that Secure Erase will be used for their private cloud. No details were available regarding this capability's implementation in their public cloud.

ii. Purpose: To sanitize data when deleting it from storage drives.

iii. Additional Guidance: While leveraging a commercial data deletion service provides the ability to securely delete data from active data on an organization's private cloud, it will not be able to delete the data that is back-up and/or distributed by the cloud provider. It's recommended that the Secure Erase is compatible with NIST 800-88. It is also recommended to leverage data encryption and strong access controls such that any data remnants that remain in backup or data distribution centers is difficult to recover by an adversary.

g. Direct Access to CSP

i. Implementation: A commercial cloud direct connect service will be leveraged by Agency #3 to connect the Agency's private cloud directly to its public cloud, thus bi-passing the ISP and creating a virtual interface between both clouds.

ii. Purpose: To provide data security between the clouds and to reduce bandwidth costs.

4. Email Protections

a. **DLP (Data Loss Prevention)**

i. Implementation: Agency #3 will subscribe to a commercial cloud data loss prevention service within their email architecture to protect against the loss of data through email.

ii. Purpose: To protect against accidental or malicious data leakage from the network.

b. **E^3A**

i. Implementation: Agency #3 plans to leverage the E^3A email protection service provided by DHS for additional email security.

ii. Purpose: To maintain compliance with Federal Government email security standards and to protect themselves from certain email threats.

c. **Additional Email Inspections**

i. Implementation: In addition to E^3A email protections, Agency #3 will leverage email protections from two their party commercial cloud services to ensure email authenticity, perform spam, phishing and imposter detection, to perform attachment inspection and other security measures.

ii. Purpose: To protect the Agency from various threat through email.

5. **Logging**
    a. **Host and Device Monitoring**
        i. Implementation: Host and device monitoring is accomplished via Agency #3's Agency-net security controls and logging that consists of syslog and cloud-based logging facilities. The Agency also uses additional tools that can be configured to monitor hosts and devices.

        ii. Purpose: To inventory hosts and devices while monitoring behavior, changes, and activity of all hosts and devices.

        iii. Additional Guidance: Commercial cloud services leveraged by Agency #3 to perform configuration management can also be leveraged for host and device monitoring as well. It is recommended that these services be leveraged for both security purposes.

6. **Configuration Management**
    a. **Device Configuration Integrity Verification**
        i. Implementation: According to CSP policy, all hybrid cloud devices will be periodically scanned using two commercial services. Agency #3's implementation diagrams indicate it has three additional commercial services that also can check and maintain the configurations of hosts and devices.

        ii. Purpose: to leverage vulnerability scanning tools to verify the integrity of device configurations within the environment.

        iii. Additional Guidance: Commercial cloud services leveraged by Agency #3 to perform configuration management can also be leveraged for device configuration integrity verification. It is recommended that these services be leveraged for both security purposes.

Cloud Security Considerations

A critical element of a cloud security baseline includes security guidelines and recommendations that directly address known and theorized threats to data security in the commercial cloud environment. This section of the cloud security baseline considers the known and theorized open-source cyber threats to data in a cloud environment, and describes security guidelines and recommendations that have the potential to mitigate those threats. In addition, this baseline also considers security vulnerabilities that can impact cloud data security that result from environment characteristics unique to the commercial cloud.

When an Agency transitions from an on-premises network environment to a commercial cloud, the Agency retains ownership of the data security risks, despite transferring data management to CSPs. Similar to traditional, on-premises networks, known and theorized malicious cyber threats are present in commercial cloud environments. Advanced persistent threats (APTs), distributed denial of service attacks (DDoS), and the impacts of stolen credentials are examples of malicious activities that can apply to on-premises and to cloud-based environments. Novel malicious activities have emerged specific to the virtual aspect of the commercial cloud environment, such as virtual machine (VM) escape.

In addition to threats to data in the cloud that originate from malicious activities, characteristics of the commercial cloud environment can create new avenues that have the potential to impact data security in the cloud environment. For example, if an organization transitions their data and applications to a commercial cloud service provider in a multitenant environment, malicious activity can reside alongside that organization's data on the same hardware. Multitenancy could be considered a cloud characteristic, or cloud business model, rather than a malicious threat; however it does present a new avenue for malicious events to occur. Cloud characteristics such as multitenancy are cloud architectural elements and commercial business model elements rather than risks to data, by definition.

Specifically with regards to cyber, NIST SP 800-53 articulates the foundational elements of risk, threat, vulnerability, and consequence as the following:[6]

> ***Risk**: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.*
>
> ***Threat**: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.*

[6] NIST SP 800-53

> ***Vulnerability**: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.*
>
> ***Consequence**: The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.*

Recommendations and guidance that address commercial cloud malicious threats and address risks to data that stem from characteristics of the commercial cloud are included as a part of the cloud security baseline articulated in this document. Due to the fact that not all of the elements included in this portion of the cloud security baseline are threats, risks, or vulnerabilities by strict definition, the collection of factors considered here are referred to as cloud security *considerations*. For the purposes of this cloud security guidance baseline document, a cloud security *consideration* is defined as:

> *Any circumstance or event arising from the migration of a cyber system to a cloud environment with the potential to generate security risk.*

This section will describe the cloud security recommendations and guidelines associated with the cloud security considerations found in available open-source cloud computing literature sources. These baseline elements are described in the context of the NIST Cybersecurity Framework.

Initial efforts focused on creating the list of cloud security considerations. Government and non-government literature search was conducted over a period of time to gain insight into how stakeholders considered cybersecurity, with a focus on cloud security. Published catalogs and lists of cloud security risks, threats, and vulnerabilities from across industry, government, academia, and public-private organizations were reviewed to benchmark cloud security concerns across a variety of sources to make sure that as many relevant security considerations were included. Once a robust list of cloud security concerns was populated, a second literature search was performed to determine what the cloud security community recommended as mitigation strategies to address those concerns. A detailed list of the cloud security considerations and the mitigation strategies that address them can be found in Appendix A.

A complete list of the recommendations, guidance, mitigations, and technical capabilities generated by this process was extracted then condensed in order to account for overlapping concepts and discrepancies in descriptions. The individual recommendations in this revised list of cloud security guidance were then defined and mapped to the NIST Cybersecurity Framework (CSF) (current version 1.1).[7] This approach assists Agencies in adhering to the CSF while using cloud services. Cybersecurity guidance in the CSF is not tailored to cloud environments; however, the definitions associated with this list of recommendations assist Agencies dealing with this gap by highlighting unique cloud circumstances and scope.

[7] https://www.nist.gov/cyberframework/draft-version-11

NIST Cybersecurity Framework Mapping

Recommendations	Definition	NIST CSF
Redundant Cloud	A CSP may "provision and operate redundant cloud facilities at geographically diverse locations" in order to "avoid creating a single point of failure" when migrating workloads (for data, applications, etc.) between machines without impacting users. Such migrations may be due to maintenance, component failure, scaling with service usage and other reasons. NIST 800-146 Most major CSPs are likely to have this capability in place, but Agencies should still perform their due diligence in testing the CSP's services, particularly for minimizing latency and other issues.	ID.BE-5, ID.GV-3, ID.RA-4, ID.SC-2, ID.SC-4, PR.PT-5
Monitor Business Health	Because Agencies utilizing cloud services must rely on CSPs to ensure efficacy of their operations, Agencies must undertake due diligence in regularly assessing the business health of the CSPs they employ. Dependencies on 3rd party organizations are common for many Agencies; this is no different for Agencies using the cloud. Malicious events, financial mismanagement and other issues can lead to varying levels of impact on the quality of service provided by the CSP, including potential termination of service and a closing of the company.	ID.AM-5, ID.BE-4, ID.RA-4, ID.SC-2, ID.SC-4
Hybrid Cloud	Hybrid cloud is a deployment model that 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." NIST 800-146. Although hybrid cloud deployments can become complex, their proper use can serve to mitigate risks to business continuity for an Agency.	ID.AM-3, ID.BE-5, ID.GV-3, ID.RA-4, PR.DS-4, PR.IP-1
Contingency Planning	Contingency planning for continued operation of services "should be addressed as part of any organization's tactical IT plans." Dependencies on CSPs, ISPs and other providers expose Agencies to risks to their business continuity. Events such as malicious attacks, unintentional errors and natural causes can lead to cloud service disruptions. Additionally, due to growth of cloud usage, service providers that may not initially appear to be cloud dependent, may still rely on CSPs for a portion of their service. Agencies should not assume that by avoiding the cloud directly they will avoid risks associated with cloud outages. NIST 800-146	ID.BE-5, ID.GV-2, ID.GV-4, ID.SC-5, PR.AT-1, PR.AT-3, PR.IP-4, PR.IP-9, PR.PT-5, RC.RP-1

SLA Language	Service Level Agreement (SLA) language must be utilized to address areas of concern when transitioning to the cloud, this includes the specifics of security controls, maintenance, responsibilities, quality of service, service changes, notifications and alerts, termination of contract, etc. Roles and responsibilities should be clearly delineated to avoid potential issues when incidents arise that require a response from the CSP, the Agency and/or other parties.	ID.AM-6, ID.BE-4, ID.BE-5, ID.GV-2, ID.GV-3, ID.SC-3, ID.SC-4, ID.SC-5, PR.AT-2, 3, 4, 5.
Exit Strategy	A strategy to guide an Agency's exit from a CSP should be in place from the start of a cloud service and kept up to date through the period of service. This document should consider various potential situations that would require an exit from the CSP as well as possible outcomes, for example transitioning data and applications to an on-premise environment, or transitioning to a new CSP. Agencies must consider data migration processes, what tools and support the CSP can provide, timelines of events, deletion and sanitization of data as well as costs, which may include fees for terminating a cloud contract, resources required to conduct the transition, and productivity lost during the exit.	ID.BE-5, ID.RA-4, PR.DS-4, PR.IP-6, PR.IP-9
Alerting from CSP	The cloud service provider should maintain a means of quickly and securely notifying appropriate Agency personnel on a variety of topics including upcoming changes, scheduled outages, maintenance, as well as security related issues and incident detection, response and recovery. Agencies should engage with CSPs for expectations of what level of information and detail to be provided in each situation, appropriate timeframes for sending alerts following an incident or in anticipation of an event, and whether or not CSPs will alert the Agency of incidents in cases where Agency data and services were not impacted or were not believed to have been impacted.	ID.AM-3, 6, ID.GV-2, ID.RA-3, PR.AT-3, RS.CO, RS.AN-5
CSP Conducts Continuous Monitoring	Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. [NIST SP 800-137] Federal Agencies are required to deploy tools and capabilities. Cloud service providers should also have an ISCM strategy in coordination with the Agency's policy.	ID.AM-4, ID.GV-1, ID.RA-1, 2, 3, ID.SC-2, 3, DE.CM

Data Sanitization	"In order for organizations to have appropriate controls on the information they are responsible for safeguarding, they must properly safeguard used media." NIST 800-88. "Sanitization techniques including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal." NIST 800-53 MP-6. In the cloud environment, the Agency will have different levels of access to the storage media, and in some cases no access at all. Thus, the Agency must engage with the CSP in order to pursue their options for ensuring sanitization of their data, including replicated data, backups, etc., to the appropriate standards. "Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle." NIST 800-144. Please also see the recommendations: Data Encryption and Key Management and Review Security Policy of CSP to Limit Unauthorized Access to Data Remnants.	ID.GV-2, 3, 4, ID.SC-3, ID.SC-4, PR.DS-1,2,3, 5, PR.IP-6, 7, 8,
Data Export Procedure	Agencies must consider the processes required to export their data from a CSP's cloud environment. What format will the data be in? How long will the procedure take? How can Agencies verify that they have exported all of their data and catch any errors or corrupted files? Can the data be transferred to Agency storage or another CSP? Agencies should also consider the security implications for data, data backups and data remnants left in the CSP's hardware.	ID.GV-2, 3, 4, PR.DS-2, 3, PR.IP-6,
Audit and Review of Services	Agencies must consider the set of events that will be detailed in audits generated by the CSP. These can include account logons, configuration changes, password changes, or lower or higher levels of granularity. Agencies must also review the information that will be generated with these events. This may include "timestamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved and access control or flow control rules invoked." NIST 800-53 AU-3. Agencies can leverage this information to review the services provided by the CSP for a wide range of purposes, including but not limited to detecting malicious behavior, forensics, resolving operational issues, and ensuring quality of service and performance. Agencies should review the NIST 800-53 AU family of controls as well as NIST 800-146 for additional guidance on when audits are performed, internal versus external audits, informational security and privacy concerns, as well as the delivery, storage and protection of audits. Please also see the recommendations Audit for Compliance Check and Periodic Review of Service Usage.	ID.AM-1, 2, 4, 5, 6, ID.GV-2, ID.GV-3, ID.SC-2, 3, **ID.SC-4**, **PR.AC-1**, 3, **PR.PT-1**, DE.AE-1, DE.CM-6
Audit for Compliance Check	Agencies must use audits to ensure their cloud usage is in compliance with laws, regulations and standards. Audit logs can be analyzed to ensure security controls are properly implemented, data protection requirements are satisfied, and other issues of compliance unique to the Agency are met. Please also see the recommendation Audit and Review of Services for additional details.	ID.AM-6, ID.GV-2, **ID.GV-3**, ID.SC-3, **ID.SC-4**, PR.AC-

		1, **PR.PT-1**, DE.AE-1
Security Testing	Agencies should conduct regular security testing on CSP services to better understand CSP security assets and operations, identify loss of situational awareness due to latencies or incomplete attack information, and characterize consequences of web-based attacks and multi-tenancy.	ID.AM-6, ID.BE-3, ID.GV-2, PR.DS-6, PR.DS-7, DE.CM-8, DE.DP-3
Tools to Predict Onset of Failure	Cloud computing stakeholders in industry should define research methods for real-time measurement and monitoring to predict onset of catastrophic failure in cloud systems, and tools to identify failure vulnerabilities. (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-293.pdf#page=29&zoom=auto,-31,592)	PR.DS-6, PR.DS-8, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.CM-8, DE.DP-5
Awareness of Patch Management of CSP	Agencies must gain awareness of the CSP's patch management policy, including: (1) How often patches are applied? (2) How the CSP will manage emergency or critical patches? (3) That the CSP has outlined the level of testing that is required applying patches (4) Who within the CSP authorizes the application of the patches, and will the customer have any input into this through process? (5) How does the CSP ensure patches are centrally controlled, distributed, and applied? (6) Roles and responsibilities for applying key patches and updates to the various systems and platforms within CPS and where the demarcation lies for patches within the customer's systems. (Raj Samani. Jim Reavis. Brian Honan. "CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security." CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security, Syngress, 2015, pp. 104–105.) Agencies should also review NIST 800-40r3 for additional details on patch management. Please also see the recommendation Patch and Update Testing.	ID.GV-2, PR.IP-12

Data Loss Prevention Policies and Countermeasures	Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of sensitive information. A data loss prevention program must be in place to stop an Agency's sensitive data from leaving the cloud through either data leakage (loss of confidentiality), or data damage or disappearance (loss of integrity or availability). This involves both policy and countermeasures, including, discovering sensitive data wherever it resides, defining data usage policies, managing incident response, monitoring the use of sensitive data, and enforcing security policies to secure data at rest, data the endpoint, and data in motion. These policies and measures must be expanded to cover an Agency's cloud usage in coordination with the CSP.	ID.AM-1, 4, 5, ID.GV-3, PR.DS 1, 2, 3, 4, 5, PR.IP 4, 5, 6, 7, 11, PR.PT-2, DE.AE-1, 4, DE.CM.
Data Encryption and Key Management	A primary security control for restricting access to sensitive data is encryption. Agencies should use encryption keys and/or sophisticated access controls to help mitigate the risks introduced by cloud security considerations such as loss of control over data, greater potential for misconfiguration of security services, inability to verify data deletion, foreign storage of data, foreign acquisition of CSP, data leakage, etc. Please also see the recommendation Data Sanitization. (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)	PR.AC-1, 3, 4, 6, 7, PR.DS-1, 2, 5
Data Redundancy & Recovery	Data redundancy and recovery are needed to ensure access to critical data in a cloud environment. Data Redundancy in the cloud enables an Agency's ongoing access to data, applications, and other services that they operate in the cloud, particularly during events such as a data center service outage, a component failure, maintenance, system scaling to accommodate high traffic, etc. Data Recovery allows for an Agency to restore data, applications, and other services following a service outage, malicious compromise, or other event. Agencies must engage with the CSP to detail how this process is carried out, where backups are stored, the expected time to complete a restoration, etc. Additionally, data redundancy and recovery can potentially assist in post-event forensics, depending on the situation.	PR.IP-4, PR.IP-9, DE.AE-3, RC.RP-1, RC.IM-1, RC.IM-2
Awareness of Proper Use of Cloud	As Agencies begin transitioning to cloud services, they must ensure that IT staff, non-IT staff, and administrators are aware of the proper use and management of cloud services. Agencies should seek resources from the CSP, open source literature, other Agencies and/or generate materials in-house to educate their employees on the cloud services employed by the Agency, the scope of their usage, the proper channels for seeking authorization to use these services or to seek additional services, compliance issues, security controls, updates, incident response, etc. Additionally, this recommendation may serve to mitigate unintentional shadow IT cloud usage by staff and administrators who utilize cloud services without going through the proper channels.	ID.GV-2, ID.AM-6, PR.AT-1, PR.AT-2, PR.AT-5, PR.IP-1, PR.IP-3, PR.IP-8, PR.IP-11, DE.AE-

		1, DE.CM-3, DE.DP-1, RS.CO-1,
Training on Security Controls	In a cloud environment, the increased burden and complexity placed on IT staff as well as a greater possibility of untrained administrators introduces a greater potential for misconfiguration of security services; thus, it is critical for Agencies to ensure that IT staff and administrators have proper training on cloud security controls. Agencies should seek both external resources to improve their IT staff's knowledge of cybersecurity considerations in the cloud as well resources provided by the CSP to inform staff of the controls they offer and how to configure and manage them.	ID.GV-2, PR.AT-1, PR.AT-2, PR.AT-5, DE.AE-1, DE.CM-3, DE.DP-1, RS.CO-1
Best Practices for Security	Agencies should seek to implement best practices for security concerns throughout the process of transitioning to and using the cloud environment. This recommendation is far-reaching but intended to capture the need for an Agency's own due diligence in ensuring they incorporate best practices and standards for security in the cloud.	ID.RA-2, PR.AT-1, PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, PR.IP-7, PR.IP-11, DE.DP-5, RS.IM-1, RS.IM-2
Least and Distributed Privileges	The cloud service provider and Agency should employ the principle of least privilege, allowing only authorized access for users (and processes) which are necessary to accomplish assigned tasks in accordance with organizational mission and business functions. [NIST 800-53] Every user or process must be able to access only the information and resources and authorizations that the entity needs to perform its function, and conversely no entity can use functions that are not necessary. Additionally, the administrative and management privileges should be distributed across several user accounts.	PR.AC-4

Firewalling	Firewalls are devices or programs that control the flow of network traffic between networks or hosts employing differing security postures. [NIST 800-41] Firewalls provide an additional layer of security, and can be used anywhere (i.e. not only on a network perimeter). Firewall policies specify how firewalls handle inbound and outbound traffic. Agencies should employ firewalls with their cloud services to mitigate risks of compromise and other malicious activities.	PR.AC-3 PR.AC-5 PR.IP-1 PR.PT-4
Segmentation and Security Zones	Utilizing segmentation and setting up security zones are similar to firewalling, however, segmentation can specify policies on both network traffic and to the workload level, which is different than firewalling, which is only on network traffic. Agencies should engage with CSP to investigate options for grouping similar workloads together so that custom security policies can be applied to those areas either at the group itself or at the workload level. This allows Agencies to tailor their security to the types of data and services they are operating in the cloud. For example, an Agency may desire to group their HR services into one segment or zone and accounting in another, then apply different custom policies to enforce different levels of security for these areas.	ID.GV-4, PR.AC-5, PR.IP-1
Software Isolation	Due to multi-tenancy in the cloud environment, CSPs must ensure their clients' resources and operations are isolated from each other. Agencies should engage with the CSP to "[u]nderstand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization." NIST 800-144. This should be done to ensure adequate separation techniques are in place to provide the desired level of security for Agency resources, data, and applications.	ID.GV-3, 4, PR.AC-5, PR.IP-1
Secure Communications with CSP	The communication mechanisms between the Agency and Cloud Service Provider (e.g., email) should be secure. There should be multiple channels of communication between the Agency and the CSP so there is no single point of failure; for example, if the CSP is experiencing an outage, there should be a way to communicate to that CSP.	ID.SC-5 PR.PT-4 PR.PT-5 RS.CO

Review Physical Security Policy of CSP	Agency should review the physical security policy of the CSP in order to identify specific risks in the physical security of its external partners. This policy should include, but is not limited to, the physical operating environment of servers, enforcement of physical access authorizations at a cloud facilities, physical access logs, and changes to keys and/or combinations. Agencies should be aware that additional review will be necessary if the CSP employs additional CSPs to provide its service as each additional CSP may process or store the Agency's data. Agencies should consult the Physical and Environmental Protection Policy and Procedures as well as the Personnel Security Policy and Procedures control families of NIST 800-53 for additional guidance.	ID.AM-1 PR.AC-2 PR.AT-5 PR.IP-5 DE.CM-2
Documentation of Decisions, Controls, Configurations, etc.	Agencies should document all decisions regarding resources in the cloud (for all SaaS, PaaS, and IaaS instances and all CSPs) in order to capture security controls, security configurations and roles and responsibilities. This tracking and documentation will enable the Agency to better manage their cloud resources, identify unusual behavior and misconfigurations, and respond to incidents more readily. Retention of this information may also be required by laws, regulations, standards, and other operational requirements.	ID.AM ID.BE ID.GV
Review Security Policy of CSP to Limit Unauthorized Access to Data Remnants	Agencies must engage with their CSP to review what security controls the CSP has in place to limit unauthorized access to data remnants. This may include controls to limit data leakage, automated methods for writing over old memory in accordance with an agreed upon standard, ensuring data at rest is encrypted and keys are appropriately managed, etc. Please also see the recommendation "Data Sanitization" for additional guidance.	ID.GV-3 ID.RA-1 PR.DS-3 PR.IP-5 PR.IP-6
Seek FedRAMP Compliant CSPs	Agencies should use cloud offerings that are FedRAMP compliant, wherever possible. "Agencies are required by law to protect any federal information that is collected, maintained, processed, disseminated, or disposed of by cloud service offerings, in accordance with FedRAMP requirements." (www.fedramp.gov) If an Agency seeks to use a CSP that is not FedRMAP authorized, or in the process of being authorized, the Agency will need to pursue additional steps to issue a FedRAMP authorization. During the authorization process Agencies will need to conduct a risk analysis, review the CSP security authorization package in detail, and determine if the risk posture is acceptable, among other steps. Agencies should visit www.fedramp.gov for details.	ID.BE-5 ID.GV

Agency Capability to Alert CSPs	Agencies should have the capability to alert a CSP in the event of malicious activity, vulnerability discovery, unusual or anomalous behavior, etc. as partners sharing cybersecurity responsibilities. Just as CSPs should have a means to alert Agency personnel, a similar capability should be established for the Agency to alert appropriate personnel at the CSP. This recommendation is separate from Secure Communications with CSP and Alerting from CSP as this is focused on incident response when detected by the Agency.	RS.CO-5 RS.CO-3
Engagement with CSP	Agencies should engage with the CSP as a partner in providing cybersecurity. These engagements should occur throughout the process of utilizing a cloud service, from language and clauses within the SLA, to the transition to cloud, its ongoing use and through the termination of services. CSPs can develop new security controls, streamline processes, provide additional information, address vulnerabilities and bugs, etc. Agency engagement with the CSP can facilitate these processes and improve security for the Agency.	ID.AM-6 ID.GV-2 DE.DP-1 RS.CO-1 RS.CO-4
Transition Planning and Roadmap	Agencies should have a well-defined plan and roadmap for transitioning data and applications to a Cloud Service Provider's services. The transition plan will consider how data and applications are securely moved to the cloud, new shared roles and responsibilities, resources, staffing and training required prior to and during transition, for example. Please see the recommendation Seek FedRAMP Compliant CSPs for additional guidance.	ID.AM ID.BE ID.GV ID.RA ID.RM
Access Rights and Controls	Access controls should be implemented on the management plane. Access controls should be implemented on all data and applications in the cloud. Agencies should engage with the CSP to explore options they can provide to manage accounts and enforce access restrictions. Agencies should also pursue additional controls for unsuccessful logon attempts, session termination procedures, and strong password policies, among others. Agencies should consult the Access Control family in NIST 800-53 for additional guidance.	PR.AC

Anomaly Detection	Anomaly detection refers to finding patterns in cybersecurity data that do not conform to expected behavior. This may involve network operations, data flows, or user behavior. Agencies will need to engage with their CSP to explore capabilities they can provide as well as review possible capability development within the Agency. For example, the Agency can review audit logs to catch activity at unusual hours or originating from atypical locations and then carry out an investigation. Anomaly detection carried out by the CSP and/or the Agency has the potential to mitigate malicious attacks, detect misconfigurations, and identify vulnerabilities.	DE.AE
Segregation of Duties	The segregation of duties (or separation of duties) is a best practice for securing IT systems. It refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process [NIST SP 800-14] Agencies should consider implementing segregation of duties as appropriate, or require the CSP to implement this best practice.	ID.AM-6, ID.GV-2, ID-GV.3, PR.AC-4, PR-AT.2, PR.AT-3, PR.AT-4, PR.AT-5, DE.CM-3, DE-DP.1, RS.CO-1
Periodic Review of Service Usage	Similar to the Audit and Review of Services recommendation, Agencies should review their service usage. Since CSPs often employ a cost model based up service usage, Agencies can review their charges and usage to detect anomalies, errors and malicious behavior. Agencies will need to establish a baseline of expected costs and adjust depending on changing operations, however, this can still provide valuable information to Agency for mitigating damaging events.	ID.GV-2, ID.SC-4, PR.AC-1, PR.PT-1, DE.AE-1

Verifying and Validating Images	For Agencies employing the IaaS model, users may choose to create foundational or "golden" virtual machines (VMs) based upon the tasks they intend to perform. When building new VMs based on these base images, users will need to check the integrity of the images to ensure they have not been compromised or altered in anyway, and are automatically configured with security policies and configurations the Agency desires. This concept is similar to when an organization "reimages" computers for an organization, i.e. the IT staff install an image on the newly purchased device based on a golden image they had previously created. Agencies will need to engage with the CSP to explore what tools are available to perform such verification and validation tests on their images in the cloud.	PR.AC-7, PR.DS-6
Intrusion Detection	Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. [from NIST SP 800-94] Agencies should engage with their CSP to ensure appropriate intrusion detection capabilities are in place for their cloud services and that these capabilities function appropriately. The latter may also be done through a 3rd party service.	DE.AE, DE.CM, DE.DP
Provisioning Controls	Cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [NIST SP 800-145] These capabilities can be quickly provisioned and released on an as needed basis, in some cases automatically, to scale rapidly outward and inward commensurate with demand. [MITRE Federal Cloud Security 2015] It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. [NIST SP 800-144] Agencies should engage with their CSPs (1) to implement controls to ensure cloud resources are provisioned securely, (2) to monitor their usage and (3) to identify and contain unauthorized provisioning.	ID.AM-4, ID.SC-3, 4, PR.DS-5, 6, 8, PR.IP-1, PR.PT-1, DE.AE-5, DE.CM-7, DE.DP-5.

Authentication and Credentialing	Authentication is the process of verifying the authorization of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. [NIST CSRC Glossary] A credential is evidence attesting to one's right to credit or authority [FIPS 201-2] (NIST 800-63 is a four-volume guidance for Digital Identity Guidelines.) In a cloud computing environment, two parties are required to manage Identity, Credential and Access Management without compromising security (CSA Security Guidance). Identity, Credential and Access Management (ICAM): Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources. [NIST CSRC Glossary] ICAM can't be managed solely by the customer (Agency) or the cloud provider and thus a trust relationship, designation of responsibilities, and the technical mechanics to enable them are required.	PR.AC, DE-CM-7
Establish Roles and Responsibilities for Forensics	Agencies should work with CSPs to establish roles, responsibilities and expectations for forensics. Forensics is the application of science to the law. Digital forensics is the application of science to the identification, collection, examination, and analysis, of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. [NIST] A cloud computing environment presents a number of challenges to forensics, exacerbating the technological, organizational, and legal challenge. Several of these challenges, such as those associated with data replication, location transparency, and multi-tenancy are unique to cloud computing. All roles and responsibilities for forensics must be defined and established in the contract language. [NIST NISTIR 8006]	ID.AM-6, ID-GV.2, ID-GV-3, RS-CO.1, RS.AN-3
Logs for API calls	Agencies must engage with their CSPs to ensure all API calls are logged and monitored. APIs may be supplied by the CSP, a 3rd party or developed by the Agency. By logging API calls, Agencies have visibility into which APIs calls are being made and who is initiating each call. Additionally, Agencies should closely monitor API calls, specifically API calls that add, edit or delete data or resources. This monitoring can enable an Agency to potentially mitigate malicious attacks, detect misconfigurations, and identify vulnerabilities.	ID.AM-6, ID.GV-2, ID.GV-3, ID.SC-3, ID.SC-4, PR.AC-1, PR.PT-1, DE.AE-1

API Versioning and Security	APIs perform specific tasks and because APIs can be modified, it is imperative that APIs are versioned so that users of the APIs know the inputs and expected results of each API call. APIs that are not versioned can create numerous issues from an API call not working because the input parameter requirements changed to unanticipated results causing an error in processing data. Additionally, all APIs should be secured. Some security protections include using encryption to protect the confidentiality and integrity of the inputs and outputs, API access keys to identify who is making API calls, and API authorization to ensure users making calls have proper permission. Agencies should ensure their CSPs version their APIs and have appropriate security controls in place. For example, if a user's API key is compromised, the CSP should have a process in place to suspend access via that key and issue the user a new key.	ID.GV-2, ID.RM-1, ID.SC-3, ID.SC-4, PR.AC-1, PR.AC-6, PR.AC-7, PR.AT-1, PR.AT-3, PR.DS-6
Patch and Update Testing	Agencies will need to engage with their CSPs to discuss when patches and updates will be applied, how much notice (if any) the Agency will have in advance, what details will be shared regarding the changes that have been made, and what resources and tools are available to agencies to test these changes. Agencies should conduct tests to ensure patches are operating correctly, verify changes do not lead to misconfigurations, check if new vulnerabilities or bugs have been introduced. The Agency should take the appropriate steps to ensure security issues the CSP claims to address through patches and updates are appropriately resolved, including zero-day exploits, bugs, and other vulnerabilities. Please also see the recommendation Awareness of Patch Management of CSP.	ID.GV-2, ID.RA-1, ID.SC-4, PR.AT-3, PR.DS-6, 7, PR.IP-12, DE.CM-8,
VM Escape Detection	VM escape has the potential to provide a malicious actor with far-reaching access in the cloud. Although these situations are difficult to mitigate, Agencies can take measures in advance to detect an event, slow an attacker down and reduce impact. These include: using appropriate data encryption and key management, auditing and reviewing of cloud services, and VM introspection, among others. Agencies should engage with their CSP to explore what additional tools they can provide, or are already using, to detect and contain incidents of VM escape. Appropriate response plans should be in place, both internally and in coordination with the CSP, for responding to possible incidents of VM Escape.	ID.AM-6, ID.GV-2, ID.GV-4, ID.RA-1, 3, 5, ID.SC-3, 4, 5, PR.AC-1, PR.DS-1, 2, 3, PR.IP-7, 9, 10, PR.PT-1, DE.AE, DE.CM, DE.DP, RS.RP, RS.CO,

		RS.AN, RS.MI, RS.IM
Training to Identify Phishing	Phishing attacks can provide attackers with private information, spread malware, and enable access to an Agency's network and systems. Cloud environments are not immune to these threats, particularly as phishing schemes continue to evolve. Agencies have options to mitigate these threats in the cloud: training staff on how to identify and avoid phishing attempts, conducting mock phishing-style attacks on employees for the purpose of education and awareness, utilizing CSP resources to improve email filtering and also block malicious URLs, etc. Agencies should include phishing attacks in their risk management plans and identify strategies for responding to the various types of incidents they can initialize, both internally and in coordination with their CSP.	ID.GV-4, ID.RA-1, 3, 5, ID.SC-3, 4, 5, PR.AT, PR.DS-1, 2, 5, PR.IP-7, 9, 10, 11, PR.PT-1, DE.CM, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM
VM Introspection	VM Introspection – Virtual Machine Introspection (VMI) allows the VM host to monitor and analyze the processes, applications and other services operating inside the VM as well as the configuration settings of the VM. This information can then be leveraged to detect malicious activity, ensure the VMs are meeting standards and to identify configuration changes. Agencies should engage with their CSP to understand what tools are available for VMI and how much of the process can be automated to reduce the burden on staff. Please also see the recommendation Segmentation and Security Zones.	ID.GV-3, 4, PR.AC-5, PR.IP-1, DE.AE-1, DE.CM-1

Current .govCAR Guidance for Cloud Security

DHS continues to maintain and evolve its ability to defend Federal civilian agencies from threats in cyberspace. In support of this mission goal, the Network Security Deployment (NSD) division of the Office of Cybersecurity and Communications (CS&C), designs, develops, deploys, and maintains the National Cybersecurity Protection System (NCPS) and manages the Continuous Diagnostics and Mitigation (CDM) program. In support of these programs, NSD advances a variety of technologies and other technical capabilities. NSD is leveraging a methodology called .govCAR, which is a cybersecurity capability investment portfolio prioritization tool. The .govCAR methodology maps current NSD capabilities against a suite of known cyber threats, aiming to identify areas where current capabilities are not fully addressing

the cybersecurity need. As the .govCAR effort considers the commercial cloud environment, the resulting recommendations, affirmations, and observations will be incorporated into this document. This section describes the currently available cloud-related .govCAR findings that apply to the baseline and links them back to existing baseline security elements where possible.

.govCAR cloud-related SPIN 3 Recommendations

1. ***Supplement the review of the FedRAMP compliance package done prior to migrating to a CSP-provided SaaS or IaaS with a security architecture review to understand the threat coverage provided through the implementation of the controls.***

It is possible that 1) the FedRAMP Provisional ATO incorporates risk acceptance that the Agency does not wish to accept, 2) the compliance package contains POAMs that do not provide an acceptable time frame to the Agency, or 3) the organizationally-defined control parameters supporting the P-ATO do not satisfy the security requirements of the Agency. Considering the threat framework and the Agency mission, ensure the critical threats that could be mitigated by FedRAMP controls are adequately addressed by the CSP. This review should be focused on informing the security architecture developed by the D/A security architect; this is not a compliance review for purposes of accreditation.

An Agency's cybersecurity due diligence on the part of a CSP's cybersecurity capabilities, including FedRAMP, is recommended prior to transitioning to a commercial cloud environment. Prior to transitioning to a commercial cloud, it is recommended that each Agency perform an analysis of what cybersecurity capabilities are needed and preferred, depending on the types of data and applications will be transitioned to the cloud. Each Agency may refer to the lists of cybersecurity capabilities referenced in this baseline for assistance in determining what unique cybersecurity portfolios are required to meet the needs of each Agency.

One element of commercial cloud cybersecurity is FedRAMP compliance. It is recommended that each Agency review FedRAMP controls and control meaning prior to choosing a CSP service to develop an understanding of FedRAMP controls and how they may intersect with their individual cybersecurity needs. For example, an Agency may determine that, due to policy requirements, their data must remain within the political borders of the US. Types of FedRAMP compliance do not require data to remain within US political borders. As such, this would be a topic worthy of a security-related discussion prior to transitioning data and applications to the cloud.

It is recommended that Agencies review the included cloud cybersecurity baseline options in this document to determine if there are topics of specific concern and subsequently:

- Determine whether FedRAMP addresses the concern, and
- Discuss any outstanding concerns with their prospective CSP. For specific concerns, protocols may be developed for communicating possible breaches, and how the CSP and Agency will work together to resolve it, what information will be communicated, etc.

Please refer to the following cloud security considerations for examples of this process at work.

Unknown CSP Backbone/Other Service Dependence

Lack of Insight into/Control over Supply Chain

Loss of Governance over Assets

Reduced Visibility and Control over Security Assets and Operations

2. ***Implement Device Health Check with Remediation for all cloud instances to ensure basic hygiene.*** *DHC will monitor patch and vulnerability status, configuration settings, file integrity status, whitelisting status, anti-malware status, and device control status. The remediation component will patch vulnerabilities when detected, apply configuration settings, providing anti-malware, and update software signatures*

The recommendation refers to an Agency's IaaS VM for example, running a cloud instance that is hosting a web application. Device health check capabilities can be either Agency-owned or CSP-owned. It is recommended that testing of any patch management be performed prior to patching of any actual Agency data VMs. Agencies and CSPs can decide on a specific approach to patch/management protocols. Please refer to the "Patch/Version Management Complications" cloud security consideration in Appendix A.

3. ***Implement a Web Application Firewall/Reverse Proxy in the cloud instance to protect most exposed element of the enclave, typically a web server in the cloud.*** *A WAF/RWP should be implemented at the Agency boundary to help protect those components. In order to realize the full value of a WAF/RWP, SSL inspection must be enabled and the WAF/RWP must be tuned to the applications it is protecting.*

Please refer to the "Web-Based Attack" cloud security consideration in Appendix A for further information on this topic. In addition, please refer to Agency Use case #1 for a cybersecurity capability implementation similar to leveraging a DMZ as a web application firewall. Use cases 2 and 3 also implement web application firewalls within their virtual environments. Please refer to the Agency Cloud Use Case section of this guideline document for details on web application firewalls performed by Agencies in the cloud.

4. ***Implement application whitelisting in the virtual server environment to prevent unknown applications from running.*** *If malware is able to gain access to a production server, it should not be able to execute because the OS will not find the application on the list of allowed software. Since the amount of production server software is typically limited, application whitelist mechanisms should be easier to implement than on user endpoints.*

It is recommended that, where appropriate, application whitelisting be leveraged in either a cloud environment or in an on-premises network. Execution responsibility for application whitelisting will depend on whether the Agency is leveraging a SaaS or an IaaS environment. For SaaS, the Agency must rely on the CSP for whitelisting

execution, while for IaaS the Agency is likely to be responsible for application whitelisting execution. NIST SP800-53 has detailed information on application whitelisting controls in control family CM-7(5).[8]

5. ***Implement ID Federation/RBAC/MFA to mitigate the threat of legitimate credential use by adversaries.*** *Multifactor authentication is probably the most important element of this capability because in most cases adversaries who are able to capture one credential are unable to capture a second in a timely manner. This recommendation is applicable to both IaaS and SaaS when Identification and Authentication is required for the data stored in the cloud.*

The compromise of credentials represents a cybersecurity risk to an Agency leveraging either on-premises or cloud computing resources in support of their mission. Please refer to Appendix A: "Compromise of Credentials" for a detailed analysis of this cybersecurity consideration. The recommended mitigation strategies to address the potential for credential compromise can be summarized as follows from Appendix A:

> *Agencies are recommended to leverage robust authentication approaches to mitigate the risk of compromised cloud credentials, such as multi-factor authentication. These strategies apply to usernames, passwords, and private keys.*[9]
>
> *If an Agency wishes to track login activity for potential compromises in credentials, they should request that this monitoring either be done by the CSP and reported to the Agency, or the login data should be make available to the Agency via an API so that the Agency can maintain its own login analysis capability.*
>
> *Separation of resources and duties for an Agency's commercial cloud service is recommended. For example, it is not recommended that Agencies leverage a single API key to access and to run all cloud functions. Responsibilities, and therefore credentials, should be broken up such that a single credential compromise cannot make an entire Agency's data vulnerable. This strategy does not prevent this attack, but it can limit the exposure of data and applications should this attack occur.*

Several recommended credential compromise mitigation strategies in this cloud security baseline are reflected in the above technical guidance including multi-factor authentication (MFA) and "role-based access control" or RBAC.

All three of the Agency cloud use cases integrate some form of MFA into their cloud security portfolios. Please refer to the Agency use case sections for available MFA implementation information on how Agencies have already integrated MFA, and other user/administrative authentication capabilities, into their cloud architectures.

NIST SP 800-53 provides guidance on authentication for Agencies looking for guidance on implementation. In addition, CSPs generally offer a variety of resources for authentication

[8] NIST SP 800-53
[9] http://searchcloudsecurity.techtarget.com/answer/Cloud-authentication-Whats-the-best-way-to-secure-cloud-credentials

purposes. It is recommended that each Agency review their authentication requirements based on their individual cloud computing and data security needs, and then work with their CSP to determine an appropriate suite of authentication capabilities.

In support of Agencies that are selecting cloud cybersecurity capabilities in support of TIC requirements, it should be noted that MFA is cited in the DHS TIC reference architecture in requirement TM.AU.01 as follows:

> *User authentication is implemented to comply with NIST SP 800-53 identification and authentication controls for high impact systems (FIPS 199).*[10] *Administrative access to point devices requires multi-factor authentication (OMB M-11-11).*

.govCAR recommendation # 5 also mentions that mitigation of credential compromise can "reduce the ability [for an adversary] to move laterally" [in the cloud environment]. A variety of cybersecurity challenges can arise from a multitenant environment. For a detailed analysis on these challenges, including risks associated with lateral movement within a cloud environment, please refer to Appendix A, "Increased Attack Surface due to Multitenancy."

6. ***Implement a virtual Intrusion Prevention System and virtual Firewall in the server virtual environment of the cloud to eliminate the ability of a malicious actor to gain access to the virtual servers and to move laterally in the cloud.***

Please refer to Appendix A "Increased Attack Surface due to Multitenancy" for a detailed discussion on cloud security challenges such as VM escape and other cybersecurity challenges associated with a multitenant cloud environment, however the technical recommendations for mitigating this challenge can be summarized as follows:

Segmentation is one recommended approach for addressing VM escape. Segmentation should be available at all layers for a secure multitenant environment. Especially in the case of IaaS, it is recommended that the Agency be aware of isolation provisions are available to them. Some of the capabilities that are applicable include VM segmentation and VM introspection.[11]

VM escape is a challenging consideration to address. In addition to segmentation, it is recommended that Agencies leverage data encryption to mitigate the consequences of VM escape. For Agencies using a commercial cloud service, it is recommended that Agencies follow best cybersecurity practices for encrypting their data, using their own keys and key management strategies where possible. In IaaS environments, it is recommended that Agencies leverage standard encryption approaches as described in FIPS.[12] Agencies may need to rely on CSPs to detect a VM escape event and to notify them that their data may have been affected.

Segmentation, also referred to as network isolation, is referenced in NIST SP 800-144:

[10] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
[11] http://searchcloudsecurity.techtarget.com/tip/Securing-a-multi-tenant-environment
[12] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

NIST 800-144 (Software isolation): Understand virtualization and other logical isolation techniques that the cloud provider employs in its multitenant software architecture, and assess the risks involved for the organization.[13]

With regards to virtual IPS and virtual firewall cloud security capabilities, this guidelines document includes examples of three Agencies implementing both of these capabilities in the Agency Cloud Use Case section. Please refer to this section for further detail on the implementation of these capabilities. All three use case Agencies leverage these capabilities in their cloud environments.

[13] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

III. CURRENT ENVIRONMENT: CAPABILITIES AND EXISTING GUIDANCE

Environment

This section will briefly outline key environmental factors surrounding the transition to cloud. Factors to be discussed include the drivers behind the transition to the cloud, the differentiating factors between cloud and on-premises network architectures, and the unique security concerns that are present in a cloud environment.

Agencies have been increasingly transitioning to cloud services due to policy guidance from the Federal government that promotes the cost efficiency and performance improvements gained through cloud computing. Historically, the Federal government has primarily focused on these and other issues related to the acquisition and deployment processes. Moving forward, cost and performance considerations will remain as a primary concern.

There is an increasing awareness of the need to focus on the security implications of outsourcing to cloud service providers. Current security measures and procedures are intended for perimeter-based networks, in which Agency users and data operate within networks maintained on-premises. Agencies using public cloud computing services access cloud resources from an off-premises provider. Agency users share these services with non-government users, further complicating traditional network security approaches.

With each Agency outsourcing services to one or many CSPs, cloud security has become a community issue involving Federal and non-Federal stakeholders. Achieving complex security objectives in a cloud environment calls for a community approach. Guidance on securing data in the cloud lacks maturity, and different standards exist for different business models and vary based on service type. Standards development (e.g., NIST) and procurement guidelines (e.g., GSA) have not matured into an operational set of security standards specific to the cloud. Given those realities, it is likely that DHS will need to both maintain and evolve existing capabilities, as well as create new ones.

The figure below displays a comparison between a perimeter-based .gov network architecture (left) and that of an Agency that has moved to the cloud (right). Each of the two scenarios presents the location of stored data, routes of access to the network and data taken by .gov and public users, and the location of a Trusted Internet Connection (TIC).

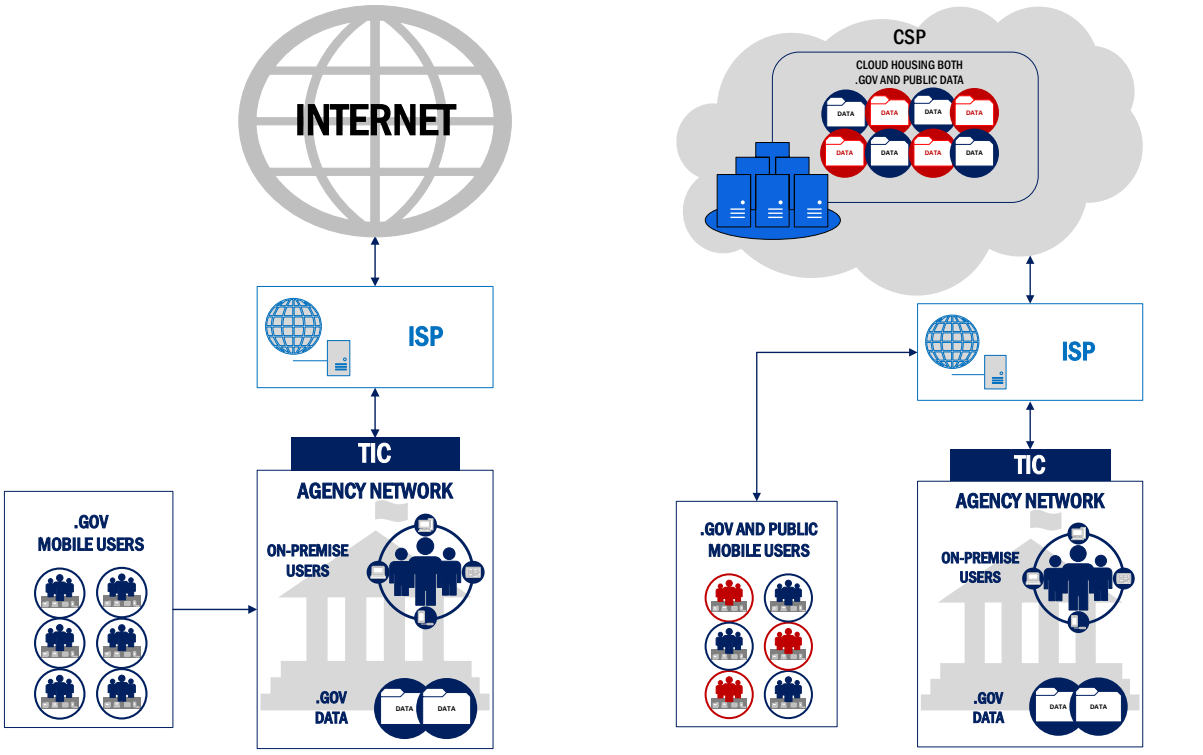


Figure 1 Perimeter-Based .gov vs. .gov Transition to Cloud

Policy Environment

The 2017 Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure[14], reinforced that Agencies own the principal responsibility of securing their data. In partnership with federal agencies across the .gov, strategic support for agency network security is distributed across several lead agencies. For example, the Department of Homeland Security (DHS) supports .gov data and network security by providing the following to Federal Agencies:

1. Protection of .gov data via a cybersecurity baseline of common capabilities (e.g., EINSTEIN, CDM) that Agencies can use to supplement their existing cybersecurity toolset,

[14] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

2. Measurement and motivation for agencies to follow best practices in cybersecurity,
3. A hub for information sharing; and,
4. Incident response assistance when an Agency suffers a cyber intrusion.

The Federal Chief Information Officer (CIO), another partner in the protection of .gov data, continues to advance the technical and policy protection capabilities for national systems.[15]

Additional stakeholders play important roles in the collection of efforts to protect .gov data. In general, the responsibility of the protection of .gov data is distributed among a community of stakeholders, each contributing unique capabilities and perspective to this complex challenge.

Key Recent Policy Developments

The White House and Congress have recently issued a series of legislation and policies aimed at modernizing Federal IT and helping agencies more effectively leverage innovative technologies, including cloud. This section summarizes recent cybersecurity legislative and policy developments and identifies takeaways relevant to agencies' cloud transition.

Recent policy developments include:

Document	Full Document Title	Summary
IT Modernization Report	*Report to the President on Federal IT Modernization*	Outlines the current and future state of Federal IT and provides immediate actions to reform the Federal government's use of IT.
NPPD Re-Organization Bill	*Cybersecurity and Infrastructure Security Agency Act*	Proposes reorganization of DHS-NPPD as an operational entity focused on protecting Federal networks and critical infrastructure.
IT Modernization Funding Bill	*Modernizing Government Technology Act*	Creates funding mechanisms that encourage agencies to retire legacy systems and procure new technologies.
National Defense Authorization Act (NDAA)	*National Defense Authorization Act for Fiscal Year 2018*	Outlines requirements for the Department of Defense and US Armed Forces, to include issues relating to cyberspace operations.
NIST Cybersecurity Framework (CSF)	*NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Draft 2)*	Revises the CSF to include more detail on self-assessment, managing external partners through supply chain risk management, and improving access controls through identity management.
National Security Strategy	*National Security Strategy of the United States of America*	Identifies US national security priorities, to include securing Federal institutions in cyberspace through IT modernization.

Key Themes

Articulating Federal IT Vision: New legislation and policy outline a future-state Federal architecture defined by shared-service deployment, data-level protection, and a risk-based security approach that prioritizes defense of high-value assets.

Emphasizing Shared Services: The White House and Congress continue to encourage agency adoption of shared services, specifically cloud services, to lower IT costs and consolidate the Federal IT model.

[15] https://www.cio.gov/agenda/cybersecurity/

Reforming IT Acquisition Processes: Recent policy and legislative developments establish new funding mechanisms and enhance existing procurement policies to accelerate agency adoption of new technologies.

Re-Affirming DHS Cyber Mission: The White House and Congress continue to affirm DHS's central role in Federal cybersecurity, designating the Department as lead on multiple government-wide modernization activities and proposing a re-organization that would allow it to more effectively execute its mission.

Impacting the SNL CS&C Portfolio: The IT Modernization Report in particular has a significant impact on the SNL CS&C portfolio, outlining a series of activities that aim to adapt flagship DHS cyber programs (e.g., NCPS, TIC, CDM) for application in cloud environments.

Report To The President On Federal It Modernization

On December 13, the White House's American Technology Council (ATC) released the finalized *Report to the President on Federal IT Modernization*, outlining the current and future state of Federal information technology (IT) and providing recommendations for immediate action to reform the Federal government's use of IT.[16,17] The ATC developed the report with support from the Department of Homeland Security (DHS), General Services Administration (GSA), White House Office of Management and Budget (OMB), and Department of Commerce (Commerce). The ATC also solicited comments from industry leaders during the month of September to gather private-sector input on the report's vision for the future of Federal IT.

Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, signed in May 2017, directed the ATC to report to the President regarding the modernization of Federal IT and required that this report describe opportunities, challenges, and effects of transitioning Federal agencies to shared IT services, as well as provide recommendations for achieving this vision.[18] A draft version of the report was released for public comment on August 30 and revised in advance of its December finalization.

Key Themes

The report's vision and recommendations generally reflect four themes:

- **Agency cloud adoption will lower costs and increase functionality**: The report echoes both EO 13800 and past Federal computing strategies by calling for agencies to transition to shared services, with cloud computing singled out for special emphasis. The ATC argues that increased use of such services will reduce Federal IT costs while maintaining and improving upon requisite levels of functionality.
- **TIC and NCPS must be overhauled to enable agency cloud migration**: The report emphasizes the shortcomings of the Federal government's perimeter- and network-based security models, and recommends transitioning the .gov architecture towards a layered defense focused on application and data-level protections. While the report does not propose discarding perimeter-based Federal

[16] American Technology Council, *Report to the President on Federal IT Modernization*, 13 December 2017. https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization.pdf
[17] Chris Liddell and Jack Wilmer, "IT Modernization," 14 December 2017. https://www.whitehouse.gov/blog/2017/12/13/final-it-modernization-report
[18] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. 5 September 2017. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

cybersecurity programs (e.g., Trusted Internet Connections (TIC), National Cybersecurity Protection System (NCPS)), it highlights the need to modify these programs in order to facilitate agency migration to the cloud and improve security.

- **IT acquisition strategy is critical to Federal IT modernization efforts**: The report positions Federal IT acquisition strategy as a critical element of modernizing the .gov's security architecture. The report presents several ways in which the Federal government can modify its IT acquisition approach to reduce inefficiencies and leverage the full purchasing power of the Federal enterprise.
- **IT modernization efforts should be guided by a common set of principles**: The report's appendices define a series of core principles that should inform future Federal IT modernization activities, as well as a series of key challenges facing DHS efforts to deliver value to agency stakeholders.[19]

Summary of Report Recommendations

The report offers two broad categories of recommendations:

1. **Network Modernization & Consolidation**: The report outlines a government-wide approach to accelerate adoption of cloud computing and modernize government-hosted applications. The report articulates a future state in which the Federal architecture is defined by cloud-optimized deployments, protection of both network perimeters and data, and a risk-based security approach that focuses agency resources on high-value assets. Specific recommendations to implement this vision include:
    - ***Prioritize the Modernization of High-Risk, High Value Assets (HVAs)***: The report recommends that the Federal government focus on enhancing security and privacy controls for the most essential and vulnerable assets within the Federal government.
    - ***Modernize the TIC and NCPS Programs to Enable Cloud Migration:*** The report recommends that the Federal government update network security policies and architectures to enable greater agency adoption of cloud services.
    - ***Consolidate Network Acquisitions and Management***: The report recommends consolidating and standardizing Federal network and security service acquisition models to reduce duplicative investments while improving situational awareness of external connections.
2. **Shared Services to Enable Future Network Architectures:** The report articulates an approach for a consolidated Federal IT model that leverages centralized technology offerings, where appropriate. Specific recommendations include:
    - ***Enable Use of Commercial Cloud Services and Infrastructures*:** The report recommends improving contract vehicles to allow agencies to acquire commercial cloud products that meet relevant security and privacy standards.
    - ***Accelerate Adoption of Cloud Email and Collaboration Tools***: The report calls for the Federal government to further support agency migration to cloud email and collaboration infrastructures.
    - ***Improve Existing and Provide Additional Security Shared Services***: The report recommends that the Federal government improve network visibility and security by providing centralized capabilities that replace or augment existing agency-specific technology.

[19] The IT Modernization Report's appendices are examined in greater length in this document's "Additional Policy Updates of Relevance" section (relevant content beginning on p. 14).

Program Impacts
The report presents recommendations and associated implementation plans with direct impact on core CS&C programs supported by SNL, including TIC, NCPS, and Continuous Diagnostics and Mitigation (CDM).

Trusted Internet Connections (TIC)

As part of its effort to promote a layered .gov security approach and emphasize application and data-level defenses, the report calls for updates to the perimeter-based TIC reference architecture (RA) and associated policies. The report outlines the following process to inform these updates:

- ***Data Call***: OMB will request information from agencies regarding cloud migration projects that have been constrained by TIC and/or NCPS policies *(within 30 days of report issuance[20]).*
- ***Categorization and Analysis***: ATC will coordinate with interagency partners (including DHS) to sort projects into three categories, each requiring different types of follow-on actions. The report also requires that OMB release a preliminary TIC policy update that formalizes the approach captured in the table below *(within 60 days of report issuance)*.

Cloud Migration Project Types and Associated Follow-On Actions

Categories	**Actions** *(to be initiated within 90 days of report issuance)*
1. Low-risk systems that can be immediately migrated to cloud.	Agencies will capture metrics and lessons learned from migration for analysis by GSA, DHS, and OMB.
2. High-priority migration candidates presenting levels of risk significant enough to require external assistance to ensure secure transfer.	GSA, DHS, OMB, National Security Council (NSC), and US Digital Service (USDS) will lead a 90-day "sprint" to validate select case studies.
3. High-risk systems that "should not be migrated until further policy direction is given or capability enhancements are made."	GSA, DHS, and OMB will work with agencies to determine whether cloud-service providers (CSPs) could provide any features or capabilities common to these systems.

- ***Policy Updates***: DHS, GSA, and OMB will use information derived from these activities to inform TIC policy updates that support agency cloud migration. Policy updates will address the following: *(within 180 days of report issuance)*

    - Lifting the current constraint of two TIC access points per agency;
    - Evaluating the impact of allowing cloud systems to not employ physical TIC protections, provided that they fulfill relevant operational-security requirements;
    - Eliminating the manual TIC Compliance Validation (TCV) process in favor of automated metrics collection; and
    - Examining options for reallocating TIC-related DHS personnel towards efforts focused on assisting agency cloud-migration efforts.

[20] The report suggests that the start date for activities is the date of issuance (December 14, 2017). However, it is unclear when these activities will officially begin, in light of the December holiday season. Internal discussions with DHS have indicated that timelines may be pushed into early January.

National Cybersecurity Protection System (NCPS)

As in the case of TIC, the report's vision of modernizing the .gov architecture requires significant changes to NCPS's current implementation. The TIC policy update process described above will also drive modifications to NCPS operational models, with a focus on the following issues:

- Clarifying the types of information traveling between agencies and commercial cloud providers that NCPS must scan;
- Identifying the NCPS capabilities most applicable in commercial cloud environments that house assets of different value;
- Identifying new NCPS capabilities that may be required in cloud environments; and
- Identifying possible modifications to the current NCPS model that would accommodate the larger number of agency access points resulting from a .gov-wide cloud transition.

Continuous Diagnostics and Mitigation (CDM)

The report validates DHS's continued expansion of the CDM program by emphasizing its role in promoting increased adoption of shared services across the Federal government. However, the report also emphasizes the need to broaden the focus of CDM to include cloud-relevant protections. Specific recommendations include:

- ***Acquisition Strategy***: The report calls for DHS to (1) finalize an acquisition strategy for task orders pertaining to CDM lifecycle support; and (2) award long-term task orders to support development and implementation of CDM Phases 3 and 4 *(within 60 days of report issuance).*
- ***CDM Shared Service Platform (SSP)***: The report calls for DHS to finalize its authority-to-operate (ATO) package with FedRAMP and submit a plan to OMB that details expectations and timelines for onboarding non-CFO Act agencies to the SSP *(within 125 days of report issuance)*.
- ***CDM Dashboards***: The report calls for DHS to (1) complete data exchanges between agency-specific and Federal dashboards, thereby "[providing] enterprise-wide situational awareness of an agency's cyber posture"; and (2) implement a Federal dashboard concept of operations (CONOPS) *(within 150 and 180 days of report issuance, respectively)*.

Differences in Workflow Capabilities in the Cloud:

Example: FedRAMP TIC-Overlay

The FedRAMP-TIC Overlay ("Overlay") was developed by FedRAMP, DHS, and an industry special interest group (SIG), with additional input from department and agency (D/A) cloud working groups. The purpose of the Overlay is to extend the perimeter-based protections of the Trusted Internet Connections initiative (TIC) to FedRAMP-certified Cloud Service Providers (CSPs) and the respective D/A users.

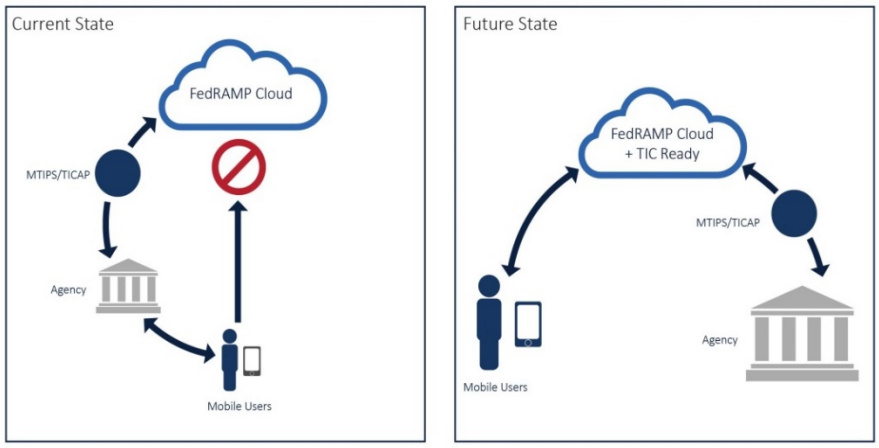


Figure X: The current and desired state for the Trusted Internet Connections initiative and Cloud Computing.

Guidance Applicable for .gov

NIST Cybersecurity Framework: The NIST Cybersecurity Framework is a voluntary set of standards and best practices intended to help organizations across the public and private sectors manage cybersecurity risks. The CSF conceptualizes five functions in the cybersecurity risk management process, outlined below.

Overview of NIST CSF Functions

Function	Definition	Categories
Identify (ID)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy
Protect (PR)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology
Detect (DE)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	• Anomalies and Events • Security Continuous Monitoring • Detection Processes
Respond (RS)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	• Response Planning • Communications • Analysis • Mitigation • Improvements
Recover (RC)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to	• Recovery Planning • Improvements • Communications

Function	Definition	Categories
	a cybersecurity event.	

APPENDIX A - Cloud Security Considerations

This section is intended to discuss, in greater detail, the individual environmental cloud considerations. For each consideration, an overview is provided to articulate why the consideration is important to consider in a commercial cloud environment, including why it requires cybersecurity attention. This section also provides references and source documentation for all considerations analyzed in this report. Below is a template consideration analysis that includes all of the analysis content that is included for each cloud consideration.

Area	Analysis	
Cloud Service Model	*SaaS* *PaaS* *IaaS*	This section will describe how each cloud consideration impacts cloud service models differently.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	This section will describe the potential consequences to, or effect on, .gov data confidentiality, integrity, and availability, if a cloud security consideration is not addressed and is exploited. • The loss of **Confidentiality** is defined as the unauthorized disclosure of information.[21] • The loss of **Integrity** is defined as the unauthorized modification or destruction of information.[22] • The loss of **Availability** is defined as the disruption of access to or use of information or an information system.[23]
	Risk to NIST Framework Implementation	This section indicates which NIST Cybersecurity Framework categories are related to the guidance provided to Agencies regarding cloud security consideration recommendations.[24]
Considerations to Guide Recommendations	This section lists questions that Agencies can use to guide SLA language and interactions with CSPs or with their internal cybersecurity groups to determine how best to protect their data in a commercial cloud environment given the Agency's specific data protection needs. Specific technical data protection guidance is not provided here due to the fact that these considerations will typically be specific to a particular Agency and data type.	
Cloud Guidance	This section articulates specific guidance that Agencies can leverage to address an environmental cloud consideration. Where possible, guidance provided here is referenced from cybersecurity guidance sources, such as the National Institute of Standards and Technology (NIST).	
Applicable FedRAMP Guidance and Controls	The Federal Risk and Authorization Management Program (FedRAMP) is designed to provide sufficient oversight and guidance to enable agencies to acquire, authorize, and use Cloud Service Offerings (CSOs) all with acceptable risk. FedRAMP processes are designed to assist Agencies in meeting FISMA requirements for cloud systems and addresses complexities of cloud systems that create unique challenges for complying with FISMA. ("Guide to Understanding FedRAMP," page 9) FedRAMP is governed by a Joint Authorization Board (JAB) comprised of the Chief Information Officers from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of	

[21] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
[22] Ibid.
[23] Ibid.
[24] https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.1-with-markup1.pdf

Area	Analysis
	Defense (DoD). The U.S. Government's Chief Information Officer Council (CIOC), including its Information Security and Identity Management Committee (ISIMC), endorses FedRAMP." (ibid., page 11) For each cloud security consideration in the tables below, the general FedRAMP process is described and particular control families from NIST 800-53 that are of higher importance to the consideration at hand are called out. These call outs emphasize particular families and are not intended to diminish other families: all the families are important. In some cases, particular controls or even control enhancements are called out. As an example, the following is provided for the first consideration: The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the Information System Contingency Plan (ISCP), which appears as Attachment 6 of the SSP, and the implementation and assessment of the controls in the Contingency Planning (CP) control family—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov. Note in the previous section the Information System Contingency Plan (ISCP) and the CP control family from NIST 800-53 that are called out. For full information on FedRAMP, go to fedramp.gov.
Supporting Data	Where possible, this section cites data or analyses that demonstrate the significance of a given cloud consideration.

Cloud Provider Outages

Overview

Regardless of their mission, Agencies must plan for unexpected service outages for IT resources and assets. Unforeseen catastrophic technological failures can render Agency services and data unavailable, unusable and possibly exposed to malicious threats.

Although commercial cloud service providers advertise service availability with minimal downtimes to consumers, service outages are inevitable due to both man-made, technological, and natural causes. When data and services are hosted by an Agency on premise, the Agency may follow previously established contingency procedures to secure the data and continue operations in the event of a catastrophic or extended service failure. However, when an Agency relies on a CSP to host their data, such events have the potential to render an Agency data, assets and service unavailable for extended periods of time without alternative options in place for restoring data, securing assets and continuing mission operations.

There are numerous examples in the open literature concerning instances of cloud services experiencing a wide array of service outages. What may be a simple error for on-site services has the potential to compound in cloud environments due to the scale at which cloud services may operate, thus, creating the potential for a far greater service failure. Failure cases range from simple email delays to authentication, configuration and administrative errors, to DDOS attacks, malware, and natural disasters that may render a service completely unavailable.

Regarding industry reliability, NIST SP 500-293 states that:

> Cloud Builders create mechanisms to compensate for component failures and deliver High Availability, but the news has highlighted major cloud provider outages. In several cases, cloud providers suffered failures or design flaws which affected the accessibility of cloud-based services for many subscribers. In April 2011, an erroneous network reconfiguration triggered a failure, followed by a cascade of recovery events and subsequent failures, and a lengthy outage. In May 2011, a sequence of cloud outages and software errors led to email delays. During June and July 2011, the same cloud provider suffered outages that disabled services. In August 2011, an intense lightning storm overloaded a power transformer; cloud services were unavailable for hours. In August 2011, a cleanup software bug resulted in customers losing backup data.

This cloud consideration is impacted by the cloud characteristics: CSP Interdependency and Distribution of Data and Many-to-One.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS* *PaaS* *IaaS*	Poses no discernable difference in its impact on the cloud service models
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	Agencies may lose access to their data or service for either limited or extended periods of time. Additionally, other entities who may need access to the Agency's data or services will also be affected.
	Risk to NIST Framework Implementation	Cloud provider outages impact Response Planning RS.RP-1and Recovery Planning RC.RP-1 as Agencies will need plans for responding to service outages and contingency plans for continuing operations.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to appropriately mitigate a loss of cloud services. • What are the roles and responsibilities of all stakeholders regarding cloud provider outages? • What tools and policies can be developed and/or are provided by a CSP to reduce downtime? • What contingency plans and redundancies does the CSP have for outages? • What interdependencies does the CSP have that could lead to an outage for the Agency (e.g. the CSP relies upon another CSP or provider for certain services necessary to run the services the Agency uses)? • Agencies must assess, "What is the frequency a duration of outages that the Agency can tolerate without adversely impacting their business processes?"[25] • Additionally, Agencies must consider, "What are the resiliency alternatives an	

[25] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

Area	Analysis
	Agency has for contingency situations involving a prolonged outage?"[26]
Cloud Guidance	Risks associated with Cloud Business Model can be addressed with the Agency's effective employment of redundant clouds, by monitoring the business health of CSPs and the use of hybrid clouds. CSPs should take steps during the entire process of design, specification, and implementation to ensure that that design flaws do not result in catastrophic failures or significant outages over extended periods of time.[27] "As USG agencies increase their use of cloud computing to provide essential services, it is essential that industry be able to ensure that design flaws do not result in catastrophic failures or significant outages over extended periods of time."[28] It is recommended that Agencies update contingency plans to cover loss or downtime of cloud services.[29] The level of availability of a cloud service and its capabilities for data backup and disaster recovery need to be addressed in the organization's contingency and continuity planning to ensure the recovery and restoration of disrupted cloud services and operations, using alternate services, equipment, and locations, if required.[30] Cloud stakeholders are recommended to formulate and publish best practices on achieving reliability.[31] Cloud stakeholders are recommended to develop a common standards for measuring and reporting industry-wide cloud reliability information to assess current and future cloud reliability.[32] Cloud stakeholders are recommended to define methods for real-time measurement and monitoring to predict onset of catastrophic failure in cloud systems, and tools to identify and avoid vulnerabilities that might lead to failure.[33] Agencies and CSPs are recommended to leverage existing industry and academic research in the area of CSP reliability, using models and current cyber threat data to discover design flaws and early indicators of service outages.[34]
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the CSP's Information System Contingency Plan (ISCP), which appears as Attachment 6 of the

[26] ibid.
[27] ibid.
[28] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-293.pdf#page=29&zoom=acontignecyuto,-31,592
[29] Ibid.
[30] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
[31] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-293.pdf#page=29&zoom=acontignecyuto,-31,592
[32] Ibid.
[33] Ibid.
[34] Ibid.

Area	Analysis
	SSP, and the implementation and assessment of the controls in the Contingency Planning (CP) control family—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	A cloud service outage at a major CSP disrupted service hundreds of thousands of clients, including some government agencies such as the CDC (February 2017).[35,36] Listing of 10 major cloud service outages and lessons learned. Article highlights how damage from Hurricane Sandy caused power outages that took servers in the region offline and impacted some major websites.[37] Lists outages from major CSPs through the year of 2017.[38] Power outage shuts down Food Stamp program, a government service that relied on a provider to verify benefits, 2013.[39] Natural disaster: "Lightning Strike Triggers CSP Outage for four hours." 2009.[40] Section 4.8 Availability of NIST 800-144 highlights additional examples of temporary, prolonged and permanent outages of cloud services.[41]

Cloud Business Model

Overview

When Agencies leverage 3rd party services for software, hardware and other needs, they are dependent upon the provider's continued business operations. If the provider changes their business model or goes out of business, the Agency must take steps to ensure data security so that their mission operations can continue.

Agencies employing cloud services are faced with the possibility that a CSP may evolve their business model, e.g., by discontinuing a previous cloud service, or may close their business operations entirely. In traditional, self-hosted environments, when physical copies of hardware, software, and other assets are purchased by an Agency, the Agency may continue to use these technologies in the event that the manufacturer or developer were to close or change their business model, e.g., a piece of software may no longer receive patches or the maker of a computer may go out of business. However, in the cloud, a change of CSP business models can reduce an Agency's available resources, change their operating environment, and pose risks to their data if too little advance warning is given in advance. An open literature search highlights instances of CSPs going out of business with little forewarning and leaving

[35] https://www.usatoday.com/story/tech/news/2017/02/28/amazons-cloud-service-goes-down-sites-scramble/98530914/
[36] http://www.latimes.com/business/technology/la-fi-tn-amazon-service-outage-20170228-story.html
[37] http://www.zdnet.com/pictures/the-10-scariest-cloud-outages-and-lessons-learned-from-them/5/
[38] http://www.crn.com/slide-shows/cloud/300089786/the-10-biggest-cloud-outages-of-2017-so-far.htm
[39] www.businessinsider.com/power-outage-shuts-down-food-stamp-program-in-17-states-2013-10
[40] http://www.datacenterknowledge.com/archives/2009/06/11/lightning-strike-triggers-amazon-ec2-outage/
[41] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

their consumers scrambling to migrate to new CSPs, secure their data, and minimize downtime for their operations.

"With on premises systems, consumers can continue to use products, even when the vendors have suspended support or have gone out of business. However, for public or outsourced cloud computing, consumers depend on near real-time provisioning of services by providers. Since business shutdown is normal in any marketplace, this dependence is a risk to consumers with time-critical computing needs."[42]

This cloud consideration is impacted by the cloud characteristics: CSP Interdependency, Distribution of Data and One-to-Many.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS*	This service model is impacted to a lesser extent than IaaS, however it can vary greatly in difficulty depending on what resources will be used. For example, if the Agency used an application through a web interface, then migration would be less difficult than if the Agency developed applications using the CSP's APIs. Migrating data and transitioning to a new authentication system will still require planning and resources but on a smaller scale than for IaaS.
	PaaS	This service model is impacted more than IaaS, but likely less than SaaS. Many of the SaaS considerations are still applicable such as potentially migrating data and ensuring correct authentication, but with PaaS a change in a platform may require a number of code changes that could range from minor alterations to significant code rewrite.
	IaaS	Transitioning services for IaaS will likely take much more planning and resources than PaaS and SaaS. This can include security infrastructure, server setups, firewall configurations, etc. that are specific to a CSP, some of which will not have an equivalent when moved to a separate service provider or may take extensive amounts of time to find an alternate solution.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	This cloud consideration has the potential to impact the availability of an Agency's data.
	Risk to NIST Framework Implementation	The Cloud Business Model consideration impacts Response Planning ID.AM and Data Security PR.DS as Agencies will need plans for identifying their data and ensuring it is securely deleted along with any backups, as well as securely transitioning their data and service to a new CSP.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to appropriately mitigate a loss of cloud services. • What are the roles and responsibilities of all stakeholders regarding a change in a CSP's business model? • What services are available to assist an Agency in migrating their data to a new CSP? • What communication does the CSP offer that gives a schedule of future changes so an Agency can plan appropriately?	

[42] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

Area	Analysis
	• In the event that a CSP terminates its services, how can an Agency securely delete their data and backups? (See analysis on "Inability to Verify Data Deletion") • How much advance notice is needed and is reasonable prior to a CSP terminating its business for an Agency to properly transition to another CSP?
Cloud Guidance	Risks associated with Cloud Business Model can be addressed with the Agency's effective employment of redundant clouds, by monitoring the business health of CSPs and the use of hybrid clouds.[43] Agency's should utilize SLA language to specify how they will retrieve their data from the CSP and ensure that it as well as any backups are sanitized. "Well documented security requirements and SLAs in CSP contracts, and open communication with the new CSP, will help to mitigate these issues. While the agency may not exit from the new CSP, the exit strategy may help to guide the change of from the old to the new CSP (in the event of a merger)."[44] "Should cloud services terminate, regardless of reason, the question of proper data handling arises. CSPs may be legally obligated to retain data and application information for a specified time period. Requests to delete cloud resources may not result in true wiping of the data. If a storage device contains data from multiple cloud consumers, (public or private sector) this is a case of multi-tenancy and hardware reuse, and potentially represents a security risk to the agency."[45] The NIST 800-35 Guide to IT Security Services includes 6 phases of the IT security life cycle, including preparing several exit strategies (Section 4.3.3).[46] Even though this is written for security services, this is applicable to any IT service.
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the Information System Contingency Plan (ISCP), which appears as Attachment 6 of the SSP, and the implementation and assessment of the controls in the Contingency Planning (CP) control family—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	In 2013, a CSP focused on data storage shut down operations.[47] "In 2008, the cloud vendor…unceremoniously ceased operations with little notice to its

[43] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
[44] https://www.mitre.org/sites/default/files/publications/pr-15-3482-cloud-security-for-federal-government.pdf
[45] Ibid.
[46] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-35.pdf
[47] https://beta.techcrunch.com/2013/09/27/its-official-the-nirvanix-cloud-storage-service-is-shutting-down/

Area	Analysis
	20,000 customers. According to [the] CEO…'at least 55% of the data was safe. How much of the remaining 45% was saved is not clear.'"[48] NIST 800-144 discusses prolonged and permanent outages, such as bankruptcy or facility loss, and cites examples beginning on page 31.[49]

Cloud Vendor Lock-In

Overview

If an Agency determines that new or alternate solutions are needed for its operations, it will move to transition services. However, when assessing the resources required to complete such a transition the Agency may find that the costs, efforts, and time may be too great and instead continue to rely on their current solutions.

For Agencies considering moving assets from one CSP to another CSP, this assessment includes reviewing data formats, proprietary APIs, high costs charged to remove presence with the original CSP, a possible inability to transfer large amounts of data out of a CSP in a timely manner, reliance on one CSP's proprietary tools, and more. The difficulties and costs associated with a transition will depend highly upon the cloud service model. If the costs are found to be high, an Agency may find it is "locked-in" with their current CSP(s).

This cloud consideration is impacted by the cloud characteristics: Distribution of Data and One-to-Many.

Analysis

Area		Analysis
Cloud Service Model Considerations	*SaaS*	The difficulty in transitioning SaaS will be far less than IaaS but may still vary greatly. See SaaS considerations for "Cloud Business Model."
	PaaS	This service model is impacted more than IaaS, but likely less than SaaS. Many of the SaaS considerations are still applicable such as potentially migrating data and ensuring correct authentication, but with PaaS a change in a platform may require a number of code changes that could range from minor alterations to significant code rewrite.
	IaaS	IaaS will be the most difficult service type to move operations from one CSP to another as Agencies will likely use many components of the CSP and will need to evaluate equivalent features of the CSP they would be moving to.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	This cloud consideration has the potential to impact the availability of an Agency's data.
	Risk to NIST Framework Implementation	The Cloud Vendor Lock-In consideration impacts Business Environment ID.BE and Risk Assessment ID.RA as Agencies will need to identify a possible dependency on a CSP(s) and the associated business impacts.

[48] www.zdnet.com/article/mediamax-the-linkup-when-the-cloud-fails/
[49] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Area	Analysis
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to appropriately mitigate a cloud vendor lock-in. • How can an Agency plan ahead for eventually leaving a CSP when entering a contract with the CSP? • How can an Agency limit its dependency on a particular CSP for the services it needs to fulfill its mission? • How can Agencies ensure data, applications and infrastructure will be able to transition to a new CSP in the future? • How and agency can evaluate the pros and cons of using CSP specific APIs vs. custom APIs written by the Agency that would be designed to be cross-platform compatible and portable to a different CSP? • When selecting a CSP for data and services, how can an Agency assess their ability to migrate large amounts of data, determine estimates for the cost of transferring out of their services and review what industry standards they meet for interoperability and portability?
Cloud Guidance	Risks associated with Cloud Vendor Lock-In can be addressed with the effective employment of redundant clouds so that an Agency can leave one CSP with a reduced disruption of services and smaller cost. An Agency should prepare a strategy for leaving a CSP in advance to minimize costs and service downtime. [50] To further reduce costs at the time of termination of services with a CSP, an Agency should require data sanitization from storage media, electronic and physical access rights be revoked from the cloud provider, and assets provided to the CSP return or, if not possible, be securely purged.[51] Agencies should consider adopting a "multicloud" solution — use two or more cloud providers, so that the Agency can leave one or the other at any time.[52] The following article provides details for recommendations to address data lock-in, application lock-in, and infrastructure lock-in.[53] As noted in Mitre's Cloud Security for Federal Government, "The agency should prepare an exit strategy as part of contracting with the CSP. This will enable the agency to plan ahead for continuity of operations in the event of a worst-case scenario."[54] The NIST 800-144 (Concluding Activities), gives a list of activities that organizations should perform when transitioning or terminating cloud services on page 50.[55] The NIST 800-35 (Guide to IT Security Services) includes 6 phases of the IT security life cycle, including preparing several exit strategies (Section 4.3.3). Although this is written for security services, it is applicable to any IT service.[56]
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the CSP's Information System Contingency Plan (ISCP), which appears as Attachment 6 of the SSP, and the implementation and assessment of the controls in the Contingency Planning (CP) control family—implies that using the CSO represents an acceptable risk, then the

[50] https://www.mitre.org/sites/default/files/publications/pr-15-3482-cloud-security-for-federal-government.pdf
[51] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
[52] https://www.cloudyn.com/blog/avoid-vendor-lock-multi-cloud-strategy/
[53] https://www.capgemini.com/2016/12/how-to-minimize-the-3-main-cloud-vendor-lock-in-risks/
[54] https://www.mitre.org/sites/default/files/publications/pr-15-3482-cloud-security-for-federal-government.pdf
[55] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
[56] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-35.pdf

Area	Analysis
	agency should be in a position to grant Authority To Operate (ATO). If need be, the agency should negotiate their contract with the CSO so that this contingency is specifically prepared for. The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	Highlights the issue and describes their own experience dealing with different data formats and lack of exporting data.[57] Articles discussing cloud vendor lock-in, examples, challenges, and mitigations.[58,59,60]

Unknown CSP Dependencies

Overview

When an Agency uses a CSP, it may be unaware of the potential of the provider to use other CSPs as part of its architecture to deliver their services, such as a SaaS-based document-sharing service that uses a major CSP's IaaS offering to store documents. The lack of visibility into these dependencies can create additional vulnerabilities and impact the Agency's reputation. Furthermore, a CSP may change their service by incorporating dependencies on additional CSPs without notifying the Agency. The impact of this risk is dependent upon the extent to which the CSP relies on other providers, e.g., to maintain/standup their services, enforce security policies, and meet compliance requirements. If a CSP relies upon additional CSPs to offer their service, these additional CSPs may suffer a service interruption which brings down services for the primary CSP or serve as an additional attack surface to compromise Agency data. An open source search of recent service outages from cloud providers will illustrate dependencies on CSPs that were not previously known. Additionally, the back-end CSP may be vulnerable to exploits, misconfigurations, or other cybersecurity risks that the Agency is unaware of with regard to their data. The loss of situational awareness regarding these dependencies creates risks for the Agency to secure their data, maintain their reputation and fulfill their mission.

This cloud consideration is impacted by the cloud characteristics: Commingling of Data, Reputational Effects, CSP Interdependency, and Distribution of Data.

Analysis

Area		Analysis
Cloud Service Model Considerations	*SaaS*	This cloud model is the most likely of three services to be impacted due to the increased chance that a SaaS provider may rely upon another CSP for portions of their service.
	PaaS	While this is more likely to impacted than IaaS, it is less likely to be impacted than SaaS.
	IaaS	This consideration is less likely to impact IaaS as the CSPs that offer such services are likely supplying the entire service without reliance on another CSP

[57] http://www.computerweekly.com/opinion/Cloud-vendor-lock-in-our-experience
[58] https://www.thorntech.com/2017/09/avoidingcloudvendorlockin/
[59] http://fortune.com/2015/10/08/aws-lock-in-worry/
[60] https://www.cloudcomputing-news.net/news/2016/sep/01/vendor-lock-in-is-big-roadblock-to-cloud-success-survey-finds/

Area	Analysis	
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	This cloud consideration has the potential to impact the confidentiality, integrity and availability of an Agency's data.
	Risk to NIST Framework Implementation	The Unknown CSP Dependencies consideration impacts Business Environment ID.BE, Risk Assessment ID.RA, and Data Security PR.DS as Agencies will need to identify a possible dependency on a CSP(s) and the associated business impacts.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to appropriately mitigate the risks associated with this consideration. • How can an Agency engage with a CSP to learn of these dependencies? Is this information available as part of a detailed FedRAMP Authorization review for a CSP? Should Agencies be required to review SOC reports in addition to FedRAMP? • How can an Agency receive notification from a CSP if the provider plans to employ an additional CSP to standup or manage its services, even if only for a limited time, e.g. in the case of a recovery operation? • How will an Agency be notified if the CSP being used as part of normal operations changes to another CSP? • What data security controls are in place regarding encryption, authentication, authorization, sanitization, etc. at each CSP involved in handling an Agency's data/applications/services?	
Cloud Guidance	Risks associated with Unknown CSP Dependencies can be addressed with the effective employment of SLAs. This is, in part, analogous to an Agency having an ISP outage or an Internet outage due to a Distributed Denial of Service attack. Agencies have to add a CSP outage to expand their traditional contingency plan. Management tools can help power through outages as applications architectures should use redundancy and data replication so that they can continue to operate in the face of outages. "The folks at Netflix have made this into a fine art, using a stateless architecture, multiple availability zones and geographical points of presence, and a robust database replication architecture to help the company's streaming service survive multiple Amazon outages. If you're simply 'lifting and shifting' old-fashioned enterprise apps from the last decade into a public cloud provider, you should expect that they will suffer the same issues as when your own data center went down, previously. Categorize your applications according to their requirements and create an appropriate strategy."[61]	
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the "Leveraged Authorizations" section of the SSP (e.g., a SaaS CSO leveraging a FedRAMP-authorized IaaS CSO)—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). If need be, the agency should negotiate their contract with the CSO so that this contingency is specifically prepared for. The agency should be attentive to the continuous and monitoring required for all CSOs. (The CSP is required to report to acquiring agencies any proposed changes to leveraged	

[61] http://www.bmc.com/blogs/six-things-you-need-to-know-about-cloud-outages/

Area	Analysis
	authorizations as part of continuous monitoring.) See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	The service outage of a major CSP in 2017 affected a number of services from other companies, especially smaller ones.[62] In 2015, an outage of CSP's service affected many companies.[63]

Lack of Insight and Control over Supply Chain

Overview

When an Agency uses a CSP, it may be unaware of the providers' supply chain management practices for mitigating risks posed by counterfeit or tampered products. The Agency may also lack insight into the providers' policies or contracts that grant additional supply chain access to outside entities for their services.

For Agencies seeking or employing cloud services from a CSP, there is a lack of insight and control over the CSP's supply chain practices for hardware, components and other technical aspects of their services. The Agencies will likely be unable to perform any form of testing on the CSP's hardware to check for compliance or reduce counterfeiting concerns, e.g. tampering, malware, spyware, quality, cost etc. The CSP may have contracts, such as maintenance contracts, with outside companies that grant these entities privileged access to various components of the services being supplied to the Agency. Thus, this cloud consideration can create vulnerabilities that grant outsiders access to compromise the confidentiality and integrity of Agency data and impact their mission. In a SaaS environment, an Agency may have very little insight into the architecture and the servers and networking used in the architecture. In PaaS and IaaS environments, the Agency should be aware of the software and versions they are using, for example the operating systems, web servers, database servers, etc., but as with a SaaS environment, the Agency will likely be unaware of the specific hardware and software used to support the services. The Agency can use SLAs to provide information and potentially add additional controls, but there is little else that can be done to mitigate the risks associated with this cloud consideration. FedRAMP controls also provide some requirements for supply chain compliances but these do not eliminate such risks entirely.

This cloud consideration is impacted by the cloud characteristics: Reputational Effects and Data Replication.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS* *PaaS* *IaaS*	All three service types are affected; however, SaaS is potentially more of a risk as a SaaS provider is more likely to be using other CSPs to support their service offerings to an Agency.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	This cloud consideration has the potential to impact the confidentiality, integrity and availability of an Agency's data. Counterfeit parts in the supply chain may lead to data corruption, theft or service outages.

[62] https://www.usatoday.com/story/tech/news/2017/02/28/amazons-cloud-service-goes-down-sites-scramble/98530914/
[63] https://aws.amazon.com/message/5467D2/

Area	Analysis	
	Risk to NIST Framework Implementation	The Lack of Insight into/Control over Supply Chain consideration impacts Risk Assessment ID.RA, supply Chain Risk Management ID.SC, Access Control PR.AC, and Data Security PR.DS.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to appropriately mitigate the risks associated with this consideration. • How can an Agency be aware of what servers, software, vendors and counterfeiting tests a CSP uses to ensure their underlying architecture is clean? • How can an Agency use SLAs to help mitigate supply chain risks? • What information is available as part of the FedRAMP authorization process?	
Cloud Guidance	The traditional model is making it unsustainable for over-stretched IT departments to keep track of the increasing complexity of components and the suppliers and the constant change in sub-components and their suppliers. With cloud computing, only the CSP needs to keep track of this for several clients and therefore can invest in a comprehensive and up-to-date strategy to do so. The Agency may not have the control that they would like to have but, realistically, they will not be able to do so themselves with the trends in complexity of infrastructure.[64,65,66]	
Applicable FedRAMP Controls	SA-12 Supply Chain Protection. (H) The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy. The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the System and Services Acquisition (SA) control family (especially control SA-12 Supply Chain Protection)—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). Control SA-12 is in the FedRAMP High baseline only. If supply chain protection is a concern for agencies, then they will need to consider only those CSO's that are authorized at the High baseline or else negotiate with CSOs to include this requirement. The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.	
Supporting Data	These various articles are not cloud specific, but they highlight how this issue pertains to computing and electronics.[67,68,69,70,71,72]	

[64] http://cerasis.com/2015/07/23/cloud-technology-in-supply-chain-management/
[65] http://www.computerweekly.com/feature/Cloud-computing-The-answer-to-supply-chain-woes
[66] https://www.forbes.com/sites/louiscolumbus/2014/02/12/where-cloud-computing-is-improving-supply-chain-performance-lessons-learned-from-scm-world/#29f34c8f67d3
[67] http://www.computerweekly.com/news/2240146742/Business-at-risk-from-fake-computer-parts
[68] https://www.computerworld.com/article/2473854/computer-hardware/counterfeit-parts-have-real-consequences.html
[69] http://www.businessinsider.com/counterfeit-parts-from-china-raise-grave-concerns-for-both-us-companies-and-national-security-2012-6

Patch and Version Management Complications

Overview

When maintaining information systems, Agencies must monitor, review and install updates and patches in order to preserve system stability and performance. These same steps are also taken to ensure security issues are appropriately addressed. Agencies need the flexibility to test and install these changes in a manner that does not impede their ability to carry out their mission. If an update, patch or other change is found to have negative consequences for the Agency, they may decide not to install them, however, they at least have the ability to make that decision. At times, mission success may require the Agency to continue to use systems that are no longer supported by vendors.

Additionally, these patches and updates can lead to new vulnerabilities that CSPs will also be responsible for addressing, e.g. a patch may be released without proper testing on the part of the CSP or may be improperly configured. Because of the reduced visibility in the cloud, Agencies may not even be aware that they are using services, software, applications, and hardware with known vulnerabilities that have not be patched.

For Agencies employing cloud services, the lack of direct control over patch and update deployments as well as the termination of services creates risks. Agencies are reliant upon the CSP to apply patches and updates to fix bugs, zero-day exploits and other security issues for vulnerable servers/services/applications in the cloud. Additionally, these patches and updates can lead to new vulnerabilities that CSPs will also be responsible for addressing, e.g. a patch may be released without proper testing on the part of the CSP or may be improperly configured. Because of the reduced visibility in the cloud, Agencies may not even be aware that they are using services, software, applications, and hardware with known vulnerabilities that have not be patched. CSPs may deploy updates and patches to their services without advanced notice in the case of a serious exploit, or it may provide little in the way of patch notes or details for the changes made. An Agency may wish to remain on a previous version of the service being offered due to software dependencies, but may not be able to run the required versions because the CSP will not allow older versions. Furthermore, even though CSPs will generally publish an update schedule, these updates may be released at a pace that is too fast for an Agency to keep up with and test against to ensure their services still function as needed to fulfill their mission space. Conversely, CSPs may react too slowly in applying patches, which may put an Agency's services or data at increased risk of comprise. Finally, if a CSP decides to abandon support for a platform or software application service, they may shut down the service entirely. In an on-premise setup, for example, an Agency may continue to run an operating system for their hardware that is no longer supported by the vendor, or the Agency may have a software application that the Agency relies upon however, in the cloud, the Agency will not have this option and will need to find an alternate solution.

This cloud consideration is impacted by the cloud characteristics: CSP Interdependency, One-to-Many, and Adaptable to Diversity of CSPs.

[70] http://money.cnn.com/galleries/2012/pf/1202/gallery.counterfeit-goods/9.html
[71] https://www.scientificamerican.com/article/the-pentagon-rsquo-s-seek-and-destroy-mission-for-counterfeit-electronics/
[72] https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS*	SaaS is less likely to be impacted by the update and patching issues since the Agency is using the CSP hosted software.
	PaaS	This is an issue with PaaS as code developed by the Agency that is dependent upon the platform will need to stay current with the CSP's upgrades/updates to the platform.
	IaaS	This is an issue with IaaS as systems created by resources provided by the CSP will need to be ready for upgrades/updates imposed by the CSP.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	This consideration can lead to a loss of confidentiality, integrity and availability of Agency data, e.g., if a software platform is abandoned or a vulnerability is left unpatched for an extended period of time.
	Risk to NIST Framework Implementation	The Patch and Version Management Complication consideration impacts Governance ID.GV, Risk Assessment ID.RA, Data Security PR.DS, Information Protection Processes and Procedures PR.IP, and Maintenance PR.MA.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to appropriately mitigate the risks associated with the lack of control over patching and version updates. For the discontinuation of a CSP's service, please refer to the cloud consideration "Cloud Business Model." • What are the responsibilities of the CSP to notify the Agency of upcoming patches, updates and service discontinuations? • Does the Agency know where the CSP publishes its patch and software version update schedule? • What tools are available to the Agency to test these changes? • For patches and updates, what details can the CSP share with the Agency to highlight what has been changed and which vulnerabilities have been addressed? • If a patch/update changes the nature of the service in such a way that the Agency can no longer achieve its goals in using the service, what options can be put in place so that the Agency can terminate service and move to another CSP? • How can Agencies notify the CSP of vulnerabilities?	
Cloud Guidance	CSA's Guide to Cloud Computing: Implementing Cloud Privacy and Security (book, 2015, page 104-105) "When engaging with a CSP the customer should make sure it is aware of what the CSP's patch management policy is. The key elements an organization should look to be included in the CSP's Patch Management Policy are (1) How often patches are applied? (2) How the CSP will manage emergency or critical patches? (3) That the CSP has outlined the level of testing that is required applying patches (4) Who within the CSP authorizes the application of the patches, and will the customer have any input into this through process? (5) How does the CSP ensure patches are centrally controlled, distributed, and applied? (6) The policy should also provide clarification as to roles and responsibilities for applying key patches and updates to the various systems and platforms within CPS and where the demarcation lies for patches within the customer's systems."[73]	

[73] Raj Samani. Jim Reavis. Brian Honan. "CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security." *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*, Syngress, 2015, pp. 104–105.

Area	Analysis
	CSA The Treacherous 12 (2016): Attacks can be mitigated with "regular vulnerability scanning, following up on reported system threats and installation of security patches or upgrades…Organizations that are highly regulated (e.g. government and financial institutions) need to be capable of handling patching quickly and, when possible, in an automatic recurring fashion. Security management must put in place a threat intelligence function, to fill the gap between the time a vulnerability is announced (known as '0-day'), and the time a patch is provided by the vendor."[74]
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the Configuration Management (CM) control family—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	Although only a few of these articles are specific to cloud, they illustrate the issues of version management.[75,76,77,78,79,80] 2014 Cyberthreat Defense Report – "75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching." Original source.[81] Spectre and Meltdown vulnerabilities.[82]

Loss of Control over Data

Overview

When storing, backing-up, transferring, and using data in an on-premise environment, Agencies have control over how, when and where these processes are performed, what security measures are implemented to protect the data and the recovery methods to be used in case of a malicious attack or catastrophic failure.

Agencies that use cloud services to handle their data do not have this same level of control over their data but are still held responsible for its protection. Data stored in the cloud can be lost due to malicious attacks, accidental deletion by users, administrators, or the cloud service provider, or a physical catastrophe such as a fire or earthquake. The burden of avoiding data loss does not rest solely on the CSP, but the loss of control over the data, the systems used for computing, storage, and transfer, "diminishes

[74] https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf
[75] https://www.csoonline.com/article/3075830/data-protection/zero-days-arent-the-problem-patches-are.html
[76] https://www.wired.com/story/equifax-breach-no-excuse/
[77] https://www.beyondsecurity.com/patching_network_vulnerabilities.html
[78] https://heimdalsecurity.com/blog/expert-roundup-software-patching/
[79] https://www.automox.com/blog/6-reasons-companies-dont-patch/
[80] https://www.ibm.com/blogs/cloud-computing/2012/02/security-patch-management-in-the-cloud/
[81] https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/rpt-cyberedge-2014-cdr.pdf
[82] https://www.cnbc.com/2018/01/03/iwhat-is-intel-chip-security-flaw-meltdown-spectre-explainer.html

the organization'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 organization."[83] Additionally, misunderstanding a CSP's storage model may result in a loss of data. An Agency must work with its CSP to understand the cloud environment they are using and ensure appropriate security measures are in place, they are in compliance with data protection laws and regulations, and data can be recovered in the result of accidental or malicious deletion. This cloud consideration has a direct impact on the availability, integrity and confidentiality of agency data and their ability to fulfill their mission. An open source search will highlight incidents where data, such as personally identifiable information (PII), were compromised through malicious attackers targeting a cloud service provider, or accidental disclosure of data.

This cloud consideration is impacted by the cloud characteristics: Commingling of Data, Distribution of Data, and CSP Interdependency.

Analysis

<table>
<tr><th>Area</th><th colspan="2">Analysis</th></tr>
<tr><td rowspan="3">Cloud Service Model Considerations</td><td>SaaS</td><td rowspan="2">Poses no discernable difference in its impact on these two cloud service models.</td></tr>
<tr><td>PaaS</td></tr>
<tr><td>IaaS</td><td>For IaaS, data recovery may be available on resources created by the Agency, however, there may be issues or restrictions with trying to recover data due to the shared resources architecture of the cloud.</td></tr>
<tr><td rowspan="2">Risk Analysis</td><td>Loss of Confidentiality, Integrity, and Availability</td><td>This cloud consideration can lead to a loss of confidentiality, integrity and availability of Agency data.</td></tr>
<tr><td>Risk to NIST Framework Implementation</td><td>The loss of control over data impacts the Identify, Protection, Detect, Respond, and Recover categories of the NIST CSF.</td></tr>
<tr><td>Considerations to Guide Recommendations</td><td colspan="2">The following questions can guide an Agency's ability to appropriately mitigate the risks associated with the loss of control over data.
What is the schedule the CSP uses for data backup? What types of backups are they (full, incremental, etc.)?
What assurances and evidence does the CSP provide that all data is encrypted while in transport and when backed-up?
If there was an accidental deletion or update of data that needed to be restored, what is the process with the CSP to restore the data?
What mechanisms are in place for encryption key management at the CSP?
What assurances does the CSP provide that certain types of data requiring strict compliance to laws and regulations are transmitted, stored, backed-up and used in compliance with the laws and regulations?
Where, geographically, does the CSP store data and back-ups? Note, "there are no FedRAMP requirements restricting data to within the United States."[84]</td></tr>
</table>

[83] https://csrc.nist.gov/publications/detail/sp/800-144/final
[84] https://www.fedramp.gov/assets/resources/documents/FedRAMP_Tips_and_Cues.pdf

Area	Analysis
Cloud Guidance	NIST 800-144 Data Protection and Availability recommendations CSA The Treacherous 12 (2016): "Cloud consumers should review the contracted data loss provisions, ask about the redundancy of a provider's solution, and understand which entity is responsible for data loss and under what conditions. Some providers offer solutions for geographic redundancy, data backup within the cloud, and premise-to-cloud backups. The risk of relying on the provider to store, backup and protect the data must be considered against handling that function in-house, and the choice to do both may be made if data is highly critical."[85]
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the Access Control (AC) control family (especially AC-4 Information Flow Enforcement), the Contingency Planning (CP) control family, and the CSP's Information System Contingency Plan (ISCP), which appears as Attachment 6 of the SSP—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	This article includes an example of data loss by a CSP when service went down.[86] CSA's The Treacherous 12: In November 2014, attackers broke into a company and leaked confidential information such as PII and email exchanges among their employees. In the first quarter 2015, the company set aside USD $15 million to address ongoing damages from the hack.[87] CSA's The Treacherous 12: In June 2014, an online hosting and code publishing provider, was hacked, leading to the compromise and complete destruction of most customer data. The company was ultimately unable to recover from this attack and went out of business.[88]

Greater Potential for Misconfiguration of Security Services

Overview

In a traditional on-premise environment, organizations must take appropriate steps to ensure IT staff and management are aware of security controls and configurations for computer systems in order to protect against vulnerabilities. The lack of a full understanding of how security controls work and/or a misconfiguration of the controls can cause systems to become vulnerable to exploitation, such as a compromise of user accounts or a data breach. In general, Agencies in an on-premise environment are

[85] https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf
[86] http://www.businessinsider.com/amazon-lost-data-2011-4
[87] http://fortune.com/sony-hack-part-1
[88] https://www.cloudcomputing-news.net/news/2014/jun/19/code-spaces-rip-code-hosting-provider-ceases-trading-after-well-orchestrated-ddos-attack/

aware of the protections they can put into place and how they are configured, e.g., firewalls, IPS, IDS, servers, etc.

This issue is magnified in the cloud due to the additional training needed to fully understand new security controls, interfaces, applications, paradigms, and vulnerabilities associated with the cloud and specific to the CSP as well as the Agency's unique needs. Additionally, a great deal of trust is placed in the CSP to implement and maintain security controls as advertised and to offer training (this could be conferences, classes, online documentation, support via email or phone call, etc.) to new tenants on how to effectively configure security controls. An unintentional misconfiguration of a system, application, or network can potentially lead to a loss of confidentiality, integrity and availability of Agency data, as well as an exposure of authentication and authorization services and other resources.

This cloud consideration is impacted by the cloud characteristics: Commingling of Data, Distribution of Data, CSP Interdependency, and Adaptable to Diversity of CSPs.

Analysis

<table>
<tr><th>Area</th><th colspan="2">Analysis</th></tr>
<tr><td rowspan="3">Cloud Service Model Considerations</td><td>SaaS</td><td rowspan="3">Poses no discernable difference in its impact on the cloud service models.</td></tr>
<tr><td>PaaS</td></tr>
<tr><td>IaaS</td></tr>
<tr><td rowspan="2">Risk Analysis</td><td>Loss of Confidentiality, Integrity, and Availability</td><td>This consideration can lead to a loss of confidentiality, integrity and availability of Agency data, e.g. sensitive data can be made available online and its confidentiality lost.</td></tr>
<tr><td>Risk to NIST Framework Implementation</td><td>This primarily impacts the Protection category of the Framework, especially Awareness and Training PR.AT, Identity Management and Access Controls PR.AC, Data Security PR.DS, and Information Protection Processes and Procedures PR.IP.</td></tr>
<tr><td>Considerations to Guide Recommendations</td><td colspan="2">The following questions can guide an Agency's ability to appropriately mitigate the risks associated with the greater potential for misconfiguration of security services.
What training is available to educate staff and management on the security services available and in use by the CSP?
What tools does a CSP provide to identify a misconfiguration of security controls?
What tools are available to the Agency to test these services, and more broadly, to what extent can an Agency verify the security services advertised by a CSP are being used appropriately?
What processes are in place to enable staff to learn from previous incidents of misconfiguration errors in order to prevent future incidents?
How frequently should an Agency conduct reviews and initiate tests to search for misconfigurations and vulnerabilities in their cloud services?
What are the default security settings implemented by the CSP?
Can misconfigurations that expose information or services publically be detected by the CSP and reported to an Agency?</td></tr>
<tr><td>Cloud Guidance</td><td colspan="2">NIST 800-144: "Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization."[89]
Additionally, Agencies will need to ensure the appropriate staff and management</td></tr>
</table>

[89] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Area	Analysis
	receive training to ensure they are knowledgeable of the applicable security controls. These same members will need to maintain an awareness of CSP services, options, settings, vulnerabilities, updates, etc. and other All data in transit or at rest in the cloud should be encrypted. Most communications to services in the cloud should be encrypted. Agencies should conduct a regular review of their systems and the services they are using either internally or in collaboration with a 3rd party service. Alerts should be established for misconfigured or potentially misconfigured security controls.
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the Access Control (AC), Awareness and Training (AT), Configuration Management (CM), and Personnel Security (PS) control families—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	Multiple Companies accidentally exposed data in the cloud.[90] Data on 15,000 patients was accidentally exposed in the cloud.[91] These articles highlight additional examples of exposed data in the cloud.[92,93]

Inability to Verify Data Deletion

Overview

Agencies using commercial cloud services may wish to remove or to delete data from a commercial cloud instance for a variety of data protection reasons including switching to a new service provider, or complying with applicable data disposal regulations or laws, among others. Subsequently, Agencies and other stakeholders may want to verify that their data has been effectively deleted.

Agencies have a greater degree of control over traceability of their data from creation to deletion and can ensure their data is sanitized to a standard of their choosing. ("Sanitization is a process to render access to target data…on the media infeasible for a given level of recovery effort."[94]) In the cloud environment data or segments of data can be distributed across multiple data centers. An Agency may never know how many backups are made nor where they are stored, much less have the ability to thoroughly wipe RAM or disks where data was located or computed.

[90] https://www.esecurityplanet.com/cloud/secure-aws-now-medical-records-accenture-data-exposed-online.html
[91] http://www.healthcareitnews.com/news/data-150000-patients-exposed-another-misconfigured-aws-bucket
[92] https://www.esecurityplanet.com/cloud/the-cloud-breach-epidemic-verizon-viacom-the-latest-to-leak-sensitive-data.html
[93] https://www.upguard.com/breaches/verizon-cloud-leak
[94] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Commercial cloud service providers may choose to distribute data across various physical or logical locations and replicate data either for load-balancing or backup purposes. These commercial cloud environmental factors create challenges for verifying data deletion, which may rely on understanding where and when data has been stored, accessed, or transmitted. In addition, verifying data deletion in the cloud involves a greater number of stakeholders to ensure and to verify that data has been deleted. An Agency may need to rely on the data tracking and data deletion procedures of a cloud service provider rather than verify that data has been deleted themselves. In addition, deletion procedures may differ from provider to provider, creating challenges for crafting a one size fits all protocol for effectively deleting Federal data.

This cloud consideration is impacted by the cloud characteristics: Distribution of Data and CSP Interdependency.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS* *PaaS* *IaaS*	Poses no discernable difference in its impact on the cloud service models.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	Agencies may not be able to verify that their data was securely deleted, and that remnants are not available to attackers. Thus, there is a potential loss of data confidentiality.[95] Adversaries can steal data remnants (e.g., passwords) to use for conducting separate attacks.
	Risk to NIST Framework Implementation	Incomplete deletion of data impacts Agency controls and capabilities in "Information Processes and Protection Procedures – PR.IP-6:Data is destroyed according to policy."
Considerations to Guide Recommendations	The following considerations can enhance an Agency's ability to ensure that their data is reliably deleted from a commercial cloud environment upon request. • What are the roles and responsibilities of all stakeholders regarding data deletion in the cloud? • What deletion standards does the CSP provide (DoD 3 pass, DoD 7 pass, etc)? • How do service providers and consumers define data deletion in the cloud? • What tools and policies can be developed and/or are provided by a CSP to mitigate this risk? • How can data deletion policies, procedures, and tools apply effectively across a diverse population of CSPs? • What data encryption and access control capabilities are available to Agencies to protect data in the cloud when relying on a commercial entity to effectively delete it? • To what extent can CSPs log and trace data in the cloud to verify data deletion? • What legal and privacy standards and regulations (e.g., HIPAA) apply to data deletion in the cloud context? • How can remnants of previously deleted data be identified?	
Cloud Guidance	Data sanitization guidelines exist from a variety of sources. Summarized here are technical recommendations for data sanitization guidelines as well as guidelines for limiting unauthorized access to data remnants should data sanitization not be completely effective. For further detail, it is recommended that stakeholders look to	

[95] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Area	Analysis
	NIST SP800-88 rev1, Guidelines for Media Sanitization, and NIST SP800-53rev4, Security and Privacy Controls for Federal Information Systems and Organizations, Appendix F-MP-6.[96,97] DOD also has data deletion guidance, e.g. DoD 5220.22-M, which articulate different levels of sanitization effort based on the sensitivity level of the data.[98] **Effective sanitization techniques**: "The application of sophisticated access controls and encryption help reduce the likelihood that an attacker can gain direct access to sensitive information."[99] The complexity will lie within the capacity of the Agency to locate and sanitize backups of data in the cloud and also to carefully manage their encryption keys. NIST 800-144 Section 4.7, Data Protection, recommends the following for Data Sanitization: "Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle."[100]
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the Media Protection (MP) control family (especially MP-6(1) MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY)—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	This research paper offers proof supporting the extistence of the threats due to data remanence in the cloud: "Experimental Proof: Data Remanence in Cloud VMs."[101]

Lack of Control over Physical Security Management

Overview

The physical security of Agency assets, data and resources is a major concern. In a traditional on-premise network environment, an Agency would have control over the physical security measures used for protecting their systems. The cloud computing environment, however, limits the Agency's ability to manage these controls as the CSP is often responsible for such actions. An Agency may find (if able to access this information at all) that a CSP's physical security measures do not meet the Agency's required/desired specifications. Poor management or implementation of these controls can lead to physical access to servers, misconfigurations, network outages, malware uploads, etc. If a CSP relies upon additional CSPs or contractors to provide services, this can increase the risk associated with this cloud consideration as each additional service provider would need to have the appropriate physical

[96] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
[97] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[98] http://www.dss.mil/documents/odaa/nispom2006-5220.pdf
[99] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
[100] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
[101] http://ieeexplore.ieee.org/document/7214152/?reload=true

security measures in place at each physical location. An Agency may not be able to influence these controls nor learn much about which controls are in place. If an adversary (who could be an insider threat, i.e., employees, or a contractor for security, electrical, HVAC, plumbing, IT support, etc.) can gain physical access to a cloud provider's hosting infrastructure, data from every organization who uses the CSP could be compromised or services could be shut down without warning.

This cloud consideration is impacted by the cloud characteristics: Distribution of Data, One-to-Many, and CSP Interdependency.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS* *PaaS* *IaaS*	Poses no discernable difference in its impact on the cloud service models.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	Poor physical security measures can lead to a loss of the confidentiality, integrity and availability of Agency data.
	Risk to NIST Framework Implementation	This consideration can impact Governance ID.GV, Identity Management, Authentication and Access Control PR.AC, Data Security PR.DS, and Security Continuous Monitoring DE.CM.
Considerations to Guide Recommendations	The following considerations can guide an Agency in reducing risks due to the lack of control over physical security management. • What are the roles and responsibilities of all stakeholders regarding physical security management? • How can Agencies engage with CSPs to review their physical security controls and management, request additional measures or updates to existing controls? • How can Agencies be alerted by a CSP when the provider experiences a breach of their physical security measures? • What additional security measures would the Agency prefer to see the CSP employ to satisfy their concerns over this consideration? • What processes are in place to notify an Agency if the CSP contracts data centers or other computing/storage facilities?	
Cloud Guidance	CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security (book, 2015, page 104-108) "Customer organizations should not take physical security controls for granted and when engaging with a CSP details of how the organization's data will be secured should be thoroughly reviewed and assessed to ensure the controls meet the requirements. This should include physical perimeter of CSP premises where controls are in place to prevent access by unauthorized personnel. The customer organization should determine that the CSP has appropriate controls in place to protect against environmental issues such as fire, floods, hurricanes, earthquakes, civil unrest or other similar threats that could disrupt services. Other physical controls should include protection against interruption to key services such as Internet access to the data centers, power, water, humidity, heat, rodent infestation, and other such threats.	

Area	Analysis
	There should be controls in place to not just prevent these threats from being realized but also to minimize their impact should they occur."[102]
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the Physical and Environmental Protection (PE) control family—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	These articles highlight a few physical security measures companies employ, some examples of events related to this consideration and a larger discussion of the issues.[103,104,105,106,107]

Foreign Storage of Data

Overview

CSPs manage data centers on a global scale. Without proper controls, Agency data may be stored, processed, etc. outside of the United States. A misconfiguration or malicious attack could lead to Agency data residing on foreign servers. Data stored in another country is subject to the jurisdiction of that country and could potentially be owned by that country. From NISTIR 7904:

Another concern with shared cloud computing is that workloads could move from cloud servers located in one country to servers located in another country. Each country has its own laws for data security, privacy, and other aspects of information technology (IT). Because the requirements of these laws may conflict with an organization's policies or mandates (e.g., laws, regulations), an organization may decide that it needs to restrict which cloud servers it uses based on their location. A common desire is to only use cloud servers physically located within the same country as the organization, or physically located in the same country as the origin of the information.[108]

Agencies will need to review the compliance and legal requirements for their data residing outside of the United States. Agencies should then engage with CSPs to ensure their data is not stored in foreign countries, as appropriate, and that their data (in transit or at rest) is encrypted so that it is protected in the event of an inadvertent or malicious redirect to a foreign server.

[102] Raj Samani. Jim Reavis. Brian Honan. "CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security." *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*, Syngress, 2015, pp. 104–108.
[103] https://www.darkreading.com/cloud/the-physical-security-factor-with-cloud-providers/d/d-id/1139075?
[104] https://blog.trendmicro.com/physical-security-cornerstone-building-safer-cloud/
[105] https://www.ibm.com/blogs/cloud-computing/2012/02/cloud-physical-security-considerations/
[106] https://www.securityindustry.org/2017/11/20/the-compelling-case-for-unifying-it-and-physical-security/
[107] https://www.csoonline.com/article/3236984/data-protection/information-security-lets-get-physical.html
[108] http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7904.pdf

This cloud consideration is impacted by the cloud characteristics: Commingling of Data, Distribution of Data, One-to-Many, and CSP Interdependency.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS* *PaaS* *IaaS*	Poses no discernable difference in its impact on the cloud service models.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	This cloud consideration can lead to a loss of confidentiality, integrity and availability of Agency data as a foreign government or other actor could render the data unavailable, claim it as their own or alter it.
	Risk to NIST Framework Implementation	This cloud consideration can impact Governance ID.IG, and Information Protection Processes and Procedures PR.IP.
Considerations to Guide Recommendations	The following considerations can guide an Agency in reducing risks due to the foreign storage of data. • What are the roles and responsibilities of all stakeholders regarding foreign storage of data? • How can Agencies engage with CSPs to filter which data centers will be used to process and store Agency data? • How can Agencies verify that their data is not being stored in foreign servers? • What data encryption and access control capabilities are available to Agencies to protect data in the cloud when relying on a commercial entity to effectively delete it? • What data security controls are in place regarding encryption, authentication, authorization, sanitization, etc. at each CSP handling Agency data/applications/services? • How can Agencies verify that certain data transmissions are not sent to foreign countries or are not routed through foreign countries?	
Cloud Guidance	NISTIR-7904 (Trusted Geolocation in the Cloud: Proof of Concept Implementation): "This provides a proof of concept solution for **IaaS** and geolocation. The proof of concept implementation is only one possible way to solve the security challenges. It is not intended to preclude the use of other products, services, techniques, etc. that can also solve the problem adequately, nor is it intended to preclude the use of any cloud products or services not specifically mentioned in this publication. The motivation behind this usage scenario is to improve the security of cloud computing and accelerate the adoption of cloud computing technologies by establishing an automated hardware root of trust method for enforcing and monitoring geolocation restrictions for cloud servers. A hardware root of trust is an inherently trusted combination of hardware and firmware that maintains the integrity of the geolocation information and the platform. The hardware root of trust is seeded by the organization, with the host's unique identifier and platform metadata stored in tamper-resistant hardware. This information	

Area	Analysis
	is accessed by management and security tools using secure protocols to assert the integrity of the platform and confirm the location of the host."[109]
Applicable FedRAMP Controls	From FedRAMP FAQ (https://www.fedramp.gov/resources/faqs/): There are no FedRAMP requirements restricting data to within the United States. There are multiple security controls that detail where data is stored, what the boundary of the system is, and where and how data in transit is protected. We have some providers that are authorized through FedRAMP that are located globally, although a majority of service providers do restrict their data to the United States. It is up to each individual agency and authorizing official to place restrictions, if needed, on data location.
Supporting Data	Although there is little in the way a CSP can do about the following incidents, these examples highlight traffic routing through countries outside of their intended pathway.[110,111,112]

Coordination with CSP for Compliance with Laws and Regulations

Overview

For Agencies operating in a traditional on-premise computing environment, they can verify if they are in compliance with various laws and regulations concerning the data they process as they are presumed to have control of the operating environment and the systems they use. However, in the cloud computing environments, Agencies often no longer have such control but are still subject to legal and regulatory requirements. Agencies must coordinate with CSPs in order to review how service providers will implement security measures and other controls so that the Agency will remain in compliance, particularly as new requirements are introduced and existing legal and regulatory conditions change. Furthermore, if a CSP relies on additional CSPs to provide their service, additional verifications and possibly SLAs must be put in place to ensure they do not fall out of compliance. Although the service provider may offer a platform that is in compliance, an Agency may still generate, process or store data on the platform in a manner that is out of compliance with legal and regulatory requirements. A few such laws and regulations include: The Federal Information Security Management Act (FISMA), the Health Information Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI DSS). Ultimately, the Agency is responsible for compliance; thus, Agencies need to review legal and regulatory requirements and work with CSPs to understand the limitations and gaps of the CSPs' offerings in this regard.

This cloud consideration is impacted by the cloud characteristics: Commingling of Data, Reputational Effects, Distribution of Data, One-to-Many, and CSP Interdependency.

Analysis

Area	Analysis	
Cloud Service Model	*SaaS*	Poses no discernable difference in its impact on the cloud service

[109] http://dx.doi.org/10.6028/NIST.IR.7904
[110] http://appleinsider.com/articles/17/12/14/intentional-event-redirects-cloud-traffic-from-apple-google-others-through-russia
[111] https://www.washingtontimes.com/news/2010/nov/15/internet-traffic-was-routed-via-chinese-servers/
[112] https://www.theverge.com/2015/3/13/8208413/uk-nuclear-weapons-russia-traffic-redirect

Area	Analysis	
Considerations	*PaaS*	models.
	IaaS	
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	The reliance on CSP and others for compliance with laws and regulations may lead to legal and financial penalties but is unlikely to lead to a loss of confidentiality, integrity or availability of Agency data.
	Risk to NIST Framework Implementation	This cloud consideration will impact Supply Chain Risk Management ID.SC, Governance ID.GV, and Information Protection Processes and Procedures PR.IP.
Considerations to Guide Recommendations	The following considerations can guide an Agency in reducing risks due to the reliance on CSPs for compliance with laws and regulations. • What are the roles and responsibilities of all stakeholders regarding regulatory and legal compliance? • What legal, regulatory and contractual requirements must the Agency be in compliance with? • How can Agencies engage with CSPs to ensure their data and service uses are in compliance with the appropriate legal and regulatory requirements? • How can Agencies verify that the CSP's services are within compliance and with what regularity? • If the CSP is not within compliance, or the Agency's use of the service is out of compliance, who is responsible for alerting the appropriate stakeholders and bringing the service, applications, data, etc. back into compliance? • What will the CSP do to ensure they meet new compliance requirements after they are introduced, e.g. through the passing of a new law? • How can Agencies keep track of the various cloud services they are using and have previously used to ensure they remain in compliance?	
Cloud Guidance	NIST 800-144: "Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which cloud providers will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf."[113] Agencies may use contract language and SLAs to ensure regular audits for compliance checks.	
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the Applicable Laws and Regulations section of the SSP (see also Attachment 12 of the SSP) is correct and that the results of the assessment implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). As soon as authorization is complete, continuous monitoring begins: To maintain an authorization that meets the FedRAMP requirements, CSPs must monitor their security controls, assess them on a regular basis, and	

[113] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Area	Analysis
	demonstrate that the security posture of their service offering is continuously acceptable. ("Continuous Monitoring Strategy Guide," Version 2.0, June 6, 2014, page 8) Presumably if a CSO meets all security controls, then it also meets the applicable laws and regulations. However, If concerns arise about the security posture of the CSP system, AOs may ask for a security artifact at any point in time. For example, if a CSP indicates in their *System Security Plan* that they actively monitor information system connections, the AO could ask the CSP to send them log file snippets for a particular connection at any point in time. If it becomes known that an entity that connects to a CSP has been compromised by an unauthorized user, the AO coordinate with the CSP to check in on the interconnection monitoring of the CSP. CSPs should anticipate that aside from scheduled continuous monitoring deliverables, and aside from testing performed by 3PAOs, that the AOs may request certain system artifacts on an ad hoc basis if there are concerns. ("Continuous Monitoring Strategy Guide," Version 2.0, June 6, 2014, page 14, emphasis in the original) For full information on FedRAMP, go to fedramp.gov.
Supporting Data	These articles provide further discussion of this consideration, recommendations to mitigate issues and lists additional federal and state laws regulating cloud activities.[114,115,116,117] Example compliance information from CSPs.[118,119,120] Examples of HIPAA Violations.[121]

Foreign Acquisition of CSP & Access to .gov

Overview

As commercial entities, cloud service providers are subject to potential mergers and acquisitions. As a result, an Agency may be leveraging cloud computing resources at a company that is bought, either partially or wholly, by another company, shifting its ownership. In some cases, the acquiring company may be a foreign company.[122]

If an Agency is still actively utilizing their cloud service when a foreign entity acquires the cloud service, or if the transaction occurs after an Agency no longer uses a cloud service but their data has not been completely deleted, the foreign entity can potentially obtain access to .gov data. The possibility of foreign entities accessing Agency data via a CSP acquisition can occur maliciously or non-maliciously. In addition, if a foreign entity has acquired CSP resources that house Agency data, a malicious third party

[114] https://www.cio.com/article/2405607/cloud-computing/cloud-computing--4-tips-for-regulatory-compliance.html
[115] http://www.informit.com/articles/article.aspx?p=1582936
[116] https://www.stratoscale.com/blog/cloud/compliance-challenge-cloud/
[117] https://www.skyhighnetworks.com/cloud-compliance/
[118] https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings
[119] https://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/
[120] https://cloud.google.com/security/compliance/eu-data-protection/
[121] https://www.skyhighnetworks.com/cloud-security-blog/hipaa-violations-examples-and-cases-8-cautionary-tales/
[122] Correspondence with DHS

can then potentially access remaining Agency data via the new ownership. CSP ownership changes can occur even if the data centers and systems are physically located within the US.

This cloud consideration is impacted by the cloud characteristics: One-to-Many, CSP Interdependency, and Adaptable to Diversity of CSPs.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS* *PaaS* *IaaS*	Poses no discernable difference in its impact on the cloud service models.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	Foreign acquisition of commercial CSPs represents a potential loss of Agency data confidentiality. If an acquisition occurs while and Agency is still leveraging its cloud services, a transfer of those services to a foreign entity may result in the loss of data confidentiality, integrity, and availability.
	Risk to NIST Framework Implementation	The foreign acquisition of a CSP impacts Identity Management, Authentication and Access Control PR.AC, Data Security PR.DS, and Information Protection Processes and Procedures PR.IP.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to appropriately mitigate a loss of cloud services. • What can Agencies do to ensure that CSPs notify them of potential or upcoming acquisitions? • What tools can CSPs provide to enable Agencies to both recover their data (or transition it to a new CSP) and to ensure the has been properly deleted. • What encryption methods are used on data? • How well are encryption keys managed?	
Cloud Guidance	CSPs should inform an Agency if part or the whole of their company is acquired by a foreign company. If a CSP is acquired by a foreign entity, the Agency should be informed with enough notice to successfully transfer their data to a new CSP, or other data center resource, in a reasonable amount of time. The CSP should to be required to work with the Agency to ensure that .gov data is securely deleted prior to acquisition by the foreign entity. (See analysis on "Inability to Verify Data Deletion")	
Applicable FedRAMP Controls	Significant changes, such as acquisition, requires prior notification of the agency by the CSP and is part of continuous monitoring: Systems are dynamic and FedRAMP anticipates that all systems are in a constant state of change. Configuration management and change control processes help maintain a secure baseline configuration of the CSP's architecture. Routine day-to-day changes are managed through the CSP's change management process described in their *Configuration Management Plan*. However, before a planned major significant change takes place, CSP's must perform a Security Impact Analysis to determine if the change will adversely affect the security of the system. The Security Impact Analysis is a standard part of a CSP's change control process as described in the CSP's *Configuration Management Plan*. CSPs must notify their AO [Authorizing Official] with a minimum of 30 days	

Area	Analysis
	before implementing any planned major significant changes. The AOs might require more time based on the severity of the change being implemented so CSPs must work close with the AOs to understand how much time is needed in advance of major changes. CSPs must complete a *Significant Change Security Impact Analysis Form* and provide to the AO for their analysis. All plans for major significant changes must include rationale for making the change, and a Security Assessment Plan (SAP) for testing the change prior to and following implementation in the production system. ("Continuous Monitoring Strategy Guide," Version 2.0, June 6, 2014, page 12, emphasis in the original) Note: The Information System Contingency Plan (ISCP) focuses on "outages, disruptions, and disasters."
Supporting Data	Although not a direct example of this issue, a recent removal of software from government Agencies highlights the threat of foreign governments obtaining data from private companies.[123,124] Other companies are suspected of sharing data with foreign governments.[125]

Increased Complexity and Burden on IT Staff

Overview

Many of the cloud security considerations in this document contain examples which highlight incidents in the cloud that have arisen due to misconfigurations, lack of training, and insufficient resources. In transitioning data and resources to the cloud, Agencies must prepare their IT staff to manage, integrate and maintain these assets in a new and different computing paradigm. The services, techniques and tools available to log and monitor assets in the cloud typically vary across CSPs, further increasing the complexity of the task. While the models available from CSPs are the same (I/S/PaaS) how each CSP architects their offering and supports them with various tools can be vastly different, requiring each Agency to investigate which is optimal for their unique mission space. This is in addition to the due diligence required to conduct a smooth and secure transition of data to the cloud in beginning the service as well as (continuously) reviewing compliance with rules, regulations, laws, best practices and computing standards. Ensuring Agency data is encrypted, logging is properly established, and appropriate access controls and authentication methods are in place in the cloud are a just a few essentials operations that require training on the part of Agency IT staff. The full extent of this training, which includes policy, management, legal, and procurement, requires time, money, and effort invested on the part of the Agency and their staff and continued engagement with the CSPs. Failure to properly train staff and prepare for operations in the cloud computing environment can lead to data breaches, misconfiguration problems, compliance issues, financial costs, etc. Agencies should understand the risks associated with going to the cloud and seek out the appropriate resources to train and assist their staff in taking on the additional burdens of IT in a cloud computing environment.

This cloud consideration is impacted by the all of the previously designated cloud characteristics.

[123] https://www.nytimes.com/2017/09/13/us/politics/kaspersky-lab-antivirus-federal-government.html
[124] https://www.washingtonpost.com/world/national-security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-f1076f6d6152_story.html?utm_term=.aa99a11c7759
[125] https://www.buzzfeed.com/sheerafrenkel/meet-the-companies-whose-business-is-letting-governments-spy?utm_term=.nsbpR5O3k#.ptqw6v781

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS*	The scope of SaaS is much smaller than the other models and therefore the SaaS model is the easiest to understand and plan properly for.
	PaaS	The scope of PaaS is limited to platforms offered by a CSP and much easier to plan and prepare for than IaaS.
	IaaS	IaaS poses the greatest concern as it provides an Agency tremendous options for customization and configuration. Much preparation must be performed to architect a secure IaaS environment.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	Failure to properly prepare for the additional burden of transitioning to and maintaining a cloud computing environment can lead to data breaches, misconfigurations and other issues that impact the confidentiality, integrity and availability of Agency data.
	Risk to NIST Framework Implementation	This cloud consideration impacts practically all aspects of the Framework.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to appropriately prepare staff for the complex challenges of operating in the cloud. • What are the various service offerings the Agency is considering in meetings its unique mission needs? • What legal, regulatory, financial and other compliance requirements must the Agency meet while employing the desired cloud service? • What resources are available to an Agency to review the process of transitioning to cloud services and maintaining these services in advance of performing such a transition? • More specifically, what training courses are available for an Agency's IT staff to prepare them for operating in the cloud environment? • What does the selected CSP offer in terms of educating their tenants on network architecture, security controls, alerting mechanisms, authentication methods, encryption schemes, logging options, etc., for their offerings? • How can staff and administrators document the decisions they have made regarding Cloud Services so as to limit the impact due to turn-over, improve efficiency, and minimize future security incidents?	
Cloud Guidance	NIST 800-144 and FedRAMP are important resources for this cloud security considerations.[126,127] CSA's Guide to Cloud Computing: Implementing Cloud Privacy and Security (book, 2015, page 114) "The people who will be working with the systems and data are a key element in maintaining the security of those systems and data. Good security requires that all staff are properly trained in how they use and interact with the systems that are using the prevent untrained people corrupting any data. Good security training should enable staff to better understand the risks involved in working with such systems and data and how they can help minimize those risks. It also requires that those charged with	

[126] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
[127] https://www.fedramp.gov/

Area	Analysis
	securing the systems and/or data are properly trained, skilled, and experienced in the technologies and the disciplines required for their role."[128] CSA's The Treacherous 12 (2016): "When executives create business strategies, cloud technologies and CSPs must be considered. Developing a good roadmap and checklist for due diligence when evaluating technologies and CSPs is essential for the greatest chance of success. An organization that rushes to adopt cloud technologies and choose CSPs without performing due diligence exposes itself to a myriad of commercial, financial, technical, legal and compliance risks that jeopardize its success."[129]
Applicable FedRAMP Controls	There is no specific FedRAMP control for this consideration. However, the FedRAMP site provides extensive material that guide the agency through the acquisition of cloud services, authorization, and the subsequent continuous monitoring phase. The intent of this material is to inform all involved, including administrators, to be able to agree, to understand, and to fulfill their various roles and responsibilities. For full information on FedRAMP, go to fedramp.gov.
Supporting Data	Articles and guides which discuss this consideration and highlight appropriate steps for planning.[130, 131, 132]

Increased Potential for Insider Threat

Overview

An insider is a current or former employee, contractor, or business partner who intentionally or unintentionally negatively affects the system or network configurations leading to a loss of confidentiality, integrity, availability, authentication or authorization.[133]

As NIST 800-144 notes, the move to a cloud environment expands the circle of potential insiders to the CSP staff and subcontractors, and also other customers using the service.[134] In comparison to an on-premise environment, this increases the potential for insiders to impact an Agency using cloud services. "From IaaS to PaaS and SaaS, a malicious insider can have increasing levels of access to more critical systems and eventually to data. Systems that depend solely on the cloud service provider (CSP) for security are at greater risk here."[135] The nature of the services offered by CSPs grants elevated privileged access to employees outside of Agencies that need to be managed effectively with proper controls. CSP and 3rd party staff with such privileged access can steal, modify, or delete Agency data, as well remove backups or transfer data to remote or foreign servers. Additionally, because an Agency has approved the use of public cloud services from the Agency's network, an employee within that Agency may use these

[128] Raj Samani. Jim Reavis. Brian Honan. "CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security." *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*, Syngress, 2015, pp. 114.
[129] https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf
[130] https://www.gartner.com/binaries/content/assets/events/keywords/catalyst/catus8/2017_planning_guide_for_cloud.pdf
[131] https://www.skyhighnetworks.com/cloud-security-blog/cio-corner-failing-to-prepare-for-cloud-is-preparing-to-fail/
[132] https://www.forbes.com/sites/forbestechcouncil/2017/06/05/13-biggest-challenges-when-moving-your-business-to-the-cloud/#73292f939b0e
[133] https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html
[134] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
[135] https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

cloud services for nefarious purposes with a decreased chance of being noticed. Agencies will need to engage with CSPs to ensure they are aware of the insider threat within their company as well as any other CSPs they may rely upon. The proper use of access controls, anomaly detection through analysis of audit logs, data loss prevention and encryption, etc., can assist in mitigating the impacts of this issue.

This cloud consideration is impacted by the cloud characteristics: Distribution of Data, One-to-Many, and CSP Interdependency.

Analysis

<table>
<tr><th>Area</th><th colspan="2">Analysis</th></tr>
<tr><td rowspan="3">Cloud Service Model Considerations</td><td>SaaS</td><td rowspan="3">There are increasing levels of access to more critical systems and data in moving from SaaS to PaaS and finally to IaaS.</td></tr>
<tr><td>PaaS</td></tr>
<tr><td>IaaS</td></tr>
<tr><td rowspan="2">Risk Analysis</td><td>Loss of Confidentiality, Integrity, and Availability</td><td>Incident arising due to insider threats have the potential to result in a loss of confidentiality, integrity, and availability of Agency data as it can be copied, modified and/or taken offline.</td></tr>
<tr><td>Risk to NIST Framework Implementation</td><td>This consideration impacts Risk Assessment ID.RA, Identify Management, Authentication and Access Control PR.AC, Data Security PR.DS, Protective Technology PR.PT, Anomalies and Events DE.AE, and Security Continuous Monitoring DE.CM.</td></tr>
<tr><td>Considerations to Guide Recommendations</td><td colspan="2">The following questions can guide an Agency’s ability to appropriately prepare staff for the complex challenges of operating in the cloud.
How aware is the CSP of the potential consequences posed by the insider threat?
What security controls are in place at the CSP to limit the potential for an insider to perpetrate an event currently?
What tools and resources are available from the CSP to identify unusual behavior in their services, either from within their company, the Agency or outside of these?
What procedures are in place at the CSP to respond to events perpetrated (intentionally or unintentionally) by an insider in their company?
What information is available in logs to investigate what actions a possible (malicious) insider may have taken?
What controls are in place to alert the CSP and/or the Agency to failed attempts to gain privileged access, to changes made to critical settings, to atypical use of resources (e.g. creating accounts), and to unusual web traffic flows.
What steps does the CSP take to review the background of employees and learn of recent criminal behavior?
How are additional 3rd parties used by either the Agency (such as a POS company or a CASB, etc.) or the CSP (electrician, HVAC, service tech, etc.) managed effectively?
How does a CSP handle the firing or letting go of an employee in terms of limiting their ability to access sensitive consumer information or impeding the quality of service offered?</td></tr>
<tr><td>Cloud Guidance</td><td colspan="2">MITRE Paper: "Contractual requirements to monitor for malicious behavior can help identify it, and SLAs can establish consequences for such insider attacks. However, the CSP’s contractual consequences of insider attack, including monetary recompense, may not even begin to repay the mission or agency consequences of the loss of sensitive government data. This added risk must be included in the agency's risk</td></tr>
</table>

Area	Analysis
	assessment of cloud solutions."[136] Encrypt data with Agency-managed keys CSA The Treacherous 12 (2016): "Implementations that use encryption provided by the CSP are still vulnerable to malicious insider attack, even though the service provider's key management duties are separated from data storage administration in mature organizations. The key finding here surrounds the CSP's auditable processes and any observations of ad hoc or less-than-measured procedures. The controls available to limit risk from malicious insiders include controlling the encryption process and keys yourself, ensuring that the CSP has proper policies; segregating duties; minimizing access by role; and effective logging, monitoring and auditing of administrators' activities."[137] CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security (book, 2015) "It is important therefore that customer organization gets assurances from the CSP that it is monitoring the insider threat and has controls in place to reduce the risk. These controls could be ensuring access controls are properly in place and maintained, there is segregation of duties clearly outlines and managed, that privileged access is granted only on a need to know basis, that access to systems is closely monitored, and that regular reviews of access rights are conducted. The CERT Insider Threat Center has additional research in this area."[138]
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the Awareness and Training (AT) and Personnel Security (PS) control families—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	NIST 800-144 gives example of a Denial of Service attack launched by a malicious insider, however, the original source links lead to Page Not Found sites. "The attack involved a cloud consumer creating an initial 20 accounts and launching virtual machine instances for each, then using those accounts to create an additional 20 accounts and machine instances in an iterative fashion, exponentially growing and consuming resources beyond set limits."[139] Additional information on insider threats for Cloud.[140,141,142,143]

[136] https://www.mitre.org/sites/default/files/publications/pr-15-3482-cloud-security-for-federal-government.pdf
[137] https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf
[138] Raj Samani. Jim Reavis. Brian Honan. "CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security." *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*, Syngress, 2015.
[139] https://csrc.nist.gov/publications/detail/sp/800-144/final
[140] https://www.bankinfosecurity.com/interviews/mitigating-insider-threat-from-cloud-i-1917
[141] https://www.skyhighnetworks.com/cloud-security-blog/5-devious-instances-insider-threat-cloud/
[142] https://securityintelligence.com/the-insider-threat-a-cloud-platform-perspective/
[143] https://blog.cloudsecurityalliance.org/2016/10/27/defeating-insider-threats-cloud/

Loss of Governance over Assets

Overview

When an agency considers transitioning some of its assets to the cloud, they will lose some governance over their assets and will need to work with their CSPs via a shared responsibility model, which will vary depending on the CSP and cloud service model. Administrators have a greater control over Agency assets in a traditional on-premise operating environment and can clearly delineate responsibilities to staff across a wide spectrum of issues. When transitioning to cloud, Agencies must understand the controls required by a FedRAMP authorization, how the CSP will meet those requirements as well as any gaps. Agencies will need to engage with the CSP to address these gaps and additional desired security features as well as to clearly delineate responsibilities through SLA, especially in instances of shared responsibilities. Agencies must understand the paradigm difference between a cloud environment and an on-premise environment, identify, understand, and manage new risks, and invest in training for staff, including training for non-technical personnel.

This cloud consideration is impacted by the cloud characteristics: Distribution of Data, One-to-Many, CSP Interdependency, One-to-Many, and Adaptable to a Diversity of CSPs.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS*	SaaS provides the least governance and control. An Agency is using applications/software provided by a CSP and has no control over the hardware or networks the application resides on.
	PaaS	PaaS like SaaS provides the least governance and control. An Agency is using platforms provided by a CSP and has no control over the hardware or networks the application resides on.
	IaaS	IaaS provides an Agency the greatest governance and control over their assets and data.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	Failure to properly prepare for the loss of governance in a cloud computing environment and clearly contracting the responsibilities of the parties involved can lead to data breaches, misconfigurations and other issues that impact the confidentiality, integrity and availability of Agency data.
	Risk to NIST Framework Implementation	This cloud consideration impacts practically all aspects of the Framework.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to appropriately prepare for the loss of governance over assets in the cloud. • What controls are provided by FedRAMP regarding the specific CSP in question? • How does the CSP implement FedRAMP controls? • What gaps exist between the CSP implementation of FedRAMP controls and the strategies and operations of the Agency? • How well does the Agency understand the new risks in moving to the cloud? • What SLAs will need to be required with CSP(s) to ensure adequate security, availability, response, recovery, etc. • What resources does the Agency have to best understand the	

Area	Analysis
	cloud environment and the impacts moving to the cloud will have across the entire Agency. • What additional security features and configurations does the Agency desire to meet their needs and remain in compliance with appropriate laws and regulations? • What resources are available to the Agency for crafting SLA language which clearly delineates responsibilities for the Agency and the CSP, more specific than shared responsibilities?
Cloud Guidance	Legal and contractual controls should be implemented to address governance issues. Security and performance must be monitored, and service providers must be auditable. Cloud computing requires greater and more thorough governance and oversight than with in-house solutions.[144]
Applicable FedRAMP Controls	With on premise hardware, agencies have physical visibility and control. With cloud, agencies have contractual control. It is not clear that the latter is "reduced." It should be at least as good: agencies should not be granting ATO to CSOs if the risk is not deemed acceptable. Depending on the agency and CSP involved, it may be enhanced. The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). For full information on FedRAMP, go to fedramp.gov.
Supporting Data	The following resources highlight important issues pertaining to the loss of governance over assets in the cloud.[145,146,147] Additionally, the following quote illustrates the impact of this cloud consideration: "Concerns about cloud service provider security have become counterproductive, and are distracting CIOs and CISOs from establishing the organizational, security and governance processes that prevent cloud security and compliance mistakes," says Heiser. "In fact, Gartner predicts that, through 2020, 95% of cloud security failures will be the customer's fault."[148]

[144] https://www.itworldcanada.com/blog/is-loss-of-control-the-biggest-hurdle-to-cloud-computing/95131
[145] http://www.gartner.com/imagesrv/books/cloud/cloud_strategy_leadership.pdf
[146] https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/IT-Governance-and-the-Cloud-Principles-and-Practice-for-Governing-Adoption-of-Cloud-Computing.aspx
[147] http://www.opengroup.org/cloud/gov_snapshot/index.htm
[148] https://scap.nist.gov/events/2009/itsac/presentations/day3/Day3_Cloud_Ritchey.pdf

Unknowledgeable Administrators

Overview

When an Agency decides to transition to cloud services, administrators who lack technical knowledge or staff who previously would not have been administrators may be responsible for leading the transition and configuring the service. Just as administrators in an on-premise environment require an appropriate level of technical knowledge in establishing on-site IT systems and network architectures, administrators who oversee or utilize cloud services need training in order to responsibly use such services. Administrators should be cautious in moving to CSPs that are not FedRAMP approved and carefully consider the implications for their Agency and their data. Since anyone can sign up for cloud service, essentially on demand, Agency employees may also seek out cloud services on their own when their IT is unable to provide them with a solution. These employees, who are now administrators of the cloud services they have setup, may then host servers and applications that are not integrated with their Agency's security standard; furthermore, there is an increased potential for misconfigured services due to a lack of knowledge on behalf of the administrators. Please see the cloud considerations Reduced Ability to Secure Unknown Agency Cloud Workloads and Greater Potential for Misconfiguration of Security Services for additional information. This consideration requires appropriate governance on behalf of the Agency. Appropriate governance and training of administrators so they can properly use cloud services in a secure way can reduce the likely of issues stemming from this consideration from occurring. An Agency's IT staff can also provide additional assistance to administrators to securely use cloud services.

This cloud consideration is impacted by the cloud characteristics: Commingling of Data, Distribution of Data, CSP Interdependency, and Adaptable to Diversity of CSPs.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS*	The scope of SaaS is much smaller than the other models and therefore the SaaS model is the easiest for administrators to understand and plan properly for.
	PaaS	The scope of PaaS is limited to platforms offered by a CSP and much easier for administrators to plan and prepare for than IaaS.
	IaaS	IaaS poses the greatest concern as it provides an Agency tremendous options for customization and configuration. Much preparation must be performed to architect a secure IaaS environment.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	Failure to properly prepare and train administrators for the additional burden of transitioning to and maintaining a cloud computing environment can lead to data breaches, misconfigurations and other issues that impact the confidentiality, integrity and availability of Agency data.
	Risk to NIST Framework Implementation	This cloud consideration impacts Asset Management ID.AM, Governance ID.GV, Risk Assessment ID.RA, Risk Management Strategy ID.RM, Identity Management, Authentication and Access Control PR.AC, Awareness and Training PR.AT, Data Security PR.DS, Information Protection Processes and Procedures PR.IP, Maintenance PR.MA, and Protective Technology PR.PT.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to appropriately prepare administrators to use cloud resources securely. • What resources are available to an Agency to educate administrators and staff	

Area	Analysis
	on transitioning to and employing cloud services? • More specifically, what training courses are available for an Agency's administrative staff to prepare them for operating in the cloud environment? • What training is available to educate staff and management on the security services available and in use by the CSP? • What does the selected CSP offer in terms of educating their tenants on network architecture, security controls, alerting mechanisms, authentication methods, encryption schemes, logging options, etc., for their offerings? • What steps can an Agency take to educate their staff on how to effectively and responsibly use cloud services? • What legal, regulatory, financial and other compliance requirements must the Agency meet while employing the desired cloud service? • Can misconfigurations that expose information or services publically be detected by the CSP and reported to an Agency? • What monitoring and controls are in place to detect when new CSP services are started within an Agency that are not approved? • What monitoring and controls are in place to detect new or modified resources or configuration settings? • What audit trails are in place to know exactly who created/modified/deleted resources or settings?
Cloud Guidance	Personnel training is very important as with adoption of any new technology. Personnel must be trained about their roles and responsibilities regarding cloud computing. CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security (book, 2015, page 114) "The people who will be working with the systems and data are a key element in maintaining the security of those systems and data. Good security requires that all staff are properly trained in how they use and interact with the systems that are using the prevent untrained people corrupting any data. Good security training should enable staff to better understand the risks involved in working with such systems and data and how they can help minimize those risks. It also requires that those charged with securing the systems and/or data are properly trained, skilled, and experienced in the technologies and the disciplines required for their role."[149]
Applicable FedRAMP Controls	The FedRAMP site provides extensive material that guide the agency through the acquisition of cloud services and the subsequent continuous monitoring phase. The intent of this material is to inform all involved, including administrators, to be able to agree, to understand, and to fulfill their various roles and responsibilities. For full information on FedRAMP, go to fedramp.gov.
Supporting Data	Please see the Supporting Data sections for the cloud security considerations "Increased Complexity and Burden on IT Staff" and "Reduced Ability to Secure Unknown Organization Cloud Workloads."

[149] Raj Samani. Jim Reavis. Brian Honan. "CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security." *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*, Syngress, 2015, pp 114.

Increased Opportunity for API Compromise

Overview

An application programming interface (API) allows programmers to interact with a system in a standardized way. The developer of the system is able to set rules, boundaries, and limit the release and use of the API. A key feature of the cloud is the abundant use of APIs, which is not typical in an on-premise environment. The purpose of their usage varies but they can enable customers to manage their cloud services and more effectively interact with their cloud applications and data, amongst other uses. Many CSPs have extensive APIs that are enabled by default and provide a user with access to the APIs that manage the entire environment. Unfortunately, as noted by the CSA "The Treacherous 12," "APIs and UIs are generally the most exposed part of a system, perhaps the only asset with an IP address available outside the trusted organizational boundary. These assets will be the target of heavy attack, and adequate controls protecting them from the Internet are the first line of defense and detection. "[150] APIs exposed by CSPs have the same software vulnerabilities that an API for an operating system, library, etc. could have, thus, malicious actors could exploit the APIs to provision, manage, and monitor assets and accounts.

Agencies will need to engage with CSPs to ensure APIs are adequately tested for security and also versioned so that Agencies can track any changes that have been made. Once more, the CSA "The Treacherous 12" explains, "API security involves more than just securing the API itself: it involves protecting API keys, cloud credentials and other sensitive data from public exposure—security measures that are sometimes overlooked by developers."[151]

This cloud consideration is impacted by the cloud characteristics: CSP Interdependency and One-to-Many, and Many-to-One.

Analysis

Area		Analysis
Cloud Service Model Considerations	*SaaS*	Depending on the CSP, APIs may be in place to either interact with the data/services from a user perspective or also the user and admin perspective. Both should be protected and understood. More damage can be done at the PaaS than the SaaS level.
	PaaS	
	IaaS	IaaS poses the greatest risk as there are many more types of resources that can be affected that can be affected by management API compromise.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	The Increased Opportunity for API Compromise may lead to a loss of confidentiality, integrity and availability of Agency data.
	Risk to NIST Framework Implementation	API compromises in the cloud may impact Risk Assessment ID.RA, Risk Management Strategy ID.RM, Identity Management, Authentication and Access Control PR.AC, Data Security PR.DS, Information Protection, Processes and Procedures PR.IP, Protective Technology PR.PT, Anomalies and Events DE.AE, Security Continuous Monitoring DE.CM, Detection Processes DE.DP, Communications RS.CO, and Analysis RS.AN.

[150] https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf
[151] Ibid.

Area	Analysis
Considerations to Guide Recommendations	The following questions can enhance an Agency's ability to mitigate risks associated with the increased opportunity for API compromise in the cloud. • How do the service providers and consumers define an incident of API Compromise in the cloud? • What are the roles and responsibilities of stakeholders regarding the disclosure of information pertaining to a compromised API in the cloud? • What ability does the Agency have to turn off APIs they don't use that are supplied by the CSP by default? • How can Agencies assess the ability of the CSP to detect and contain an incident involving a compromised API? • What security measures are in use by the CSP to protect APIs, authenticate their calls, and secure their authentication keys? • What capabilities are in place to detect malicious use of APIs? • What logging/audit trails are in place by the CSPs for APIs? • How extensible are CSPs APIs, e.g. can an Agency build APIs on top of or in addition to the CSP? If so, what testing will Agencies do to ensure the APIs are secure? • In the event of a compromised API key, what process does the CSP have in place block future its future use and issue a new key to the Agency? • What training is available to Agency staff and administrators to educate them on steps they can take to securely use APIs and help them understand the extent of APIs' reach in the service/architecture? • What tools or functionality can the CSP to limit access to APIs where they are not need? For example, if an Agency decides a set of API calls will not be used, can the CSP prevent them from being used so that in the case of an incident, the perpetrator does not have access to those calls? • Does the CSP version their APIs? If APIs change, how are Agencies notified of the changes? • What security measures are employed by the CSP regarding data loss prevention, encryption and anomaly detection to mitigate the long-term effects of this consideration?
Cloud Guidance	CSA The Treacherous 12 (2016): "Threat modeling applications and systems, including data flows and architecture/design, become important regular parts of the development lifecycle. In addition to security-specific code reviews, rigorous penetration testing becomes a requirement."[152]
Applicable FedRAMP Controls	Through the process of acquisition, the issue of protecting the channel between agency and CSP is in both of their interests and thus should be addressed to the satisfaction of both parties. During the subsequent continuous monitoring phase, the CSP is required to provide the results of extensive monitoring, including vulnerability scanning on a "continuous and ongoing" basis and a full security assessment, including a penetration test, annually (see the "Continuous Monitoring Strategy Guide" at fedramp.gov >

[152] https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

Area	Analysis
	resources > documents). For full information on FedRAMP, go to fedramp.gov.
Supporting Data	CSA The Treacherous 12: 'The IRS Breach and the Importance of Adaptive API Security – "In mid-2015, the US Internal Revenue Service (IRS) exposed over 300,000 records via a vulnerable API ("Get Transcript")." Original Source.[153] The following sources discuss API security, the threats, the impacts, and lessons learned from a related incident.[154,155,156]

Reduced Visibility and Control over Security Assets and Operations

Overview

Organizations, government or otherwise, have incentives to maintain a level of security control over data and applications due to processing and storage of sensitive data, such as personally identifiable information (PII), official use only (OUO) data, or business-sensitive (proprietary) information. Having ownership of the security infrastructure, implementation, processes, and policies that work together to protect an organization's data and assets ensures that the organization has full insight and control of those security processes and capabilities. For the purposes of this consideration, a security asset refers to hardware and associated firmware and software for security infrastructure such as sensors and firewalls. Operations refer to the processes and protocols for how those assets are used within an organization, and how they are implemented.

In the commercial cloud environment, an organization transitions their data into an environment where they no longer own the security assets and have limited control of these assets. As a result, the organization owning the data loses visibility and control over those security capabilities and processes. If an Agency transitions to the commercial cloud, they no longer have control over sensor positioning or, in some instances, firewall controls. For example, the Agency no longer has the ability to place sensors where they would like within the networks they use.

As an example of this concern from industry, at the 2015 RSA Conference, the CEO of the Cloud Security Alliance, was cited as stating that "Someone hacking…a major cloud provider is not the concern…The concern is that someone is going to gain access to your accounts, and you won't know it because it's not your infrastructure."[157]

This cloud consideration is impacted by the cloud characteristics: Distribution of Data, CSP Interdependency and One-to-Many.

Analysis

Area	Analysis	
Cloud Service Model	*SaaS*	The SaaS service model is expected to experience the greatest impact on visibility and control over security assets and

[153] http://apigee.com/about/blog/technology/irs-breach-and-importance-adaptive-api-security
[154] https://threatpost.com/protecting-cloud-apis-critical-to-mitigating-total-compromise/118197/
[155] https://www.ciosummits.com/Online_Asset_Akana_White_Paper_-_API_Security-A_Guide_To_Securing_Your_Digital_Channels.pdf
[156] https://www.entrepreneur.com/article/295831
[157] http://searchcloudsecurity.techtarget.com/news/4500243733/Cloud-visibility-a-top-concern-ahead-of-RSA-Conference-2015

Area	Analysis	
Considerations		operations, due to the Agency having the least control over the infrastructure.
	PaaS	Depending on the individual CSP, the loss of visibility and control experienced by an Agency over security assets and operations at the PaaS level will be intermediate between the IaaS and SaaS models.
	IaaS	With an IaaS service model, an Agency will have greater visibility and control over security assets and operations relative to PaaS and SaaS service models, but still less visibility and control compare to on premise networks. For example, in an IaaS, an Agency can put resources into a virtual private cloud (VPC) they create and monitor all traffic in and out of the virtual private cloud.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	Agency data compromised due to this cloud consideration can result in a loss of Confidentiality and Integrity
	Risk to NIST Framework Implementation	This cloud consideration will impact Asset Management ID.AM, Identity Management, Authentication and Access Control PR.AC, Data Security PR.DS, Information Protection Processes and Procedures PR.IP, Security Continuous Monitoring DE.CM, and Communication RS.CO.
Considerations to Guide Recommendations	The following considerations can guide an Agency through the process of determining whether a commercial cloud service's security asset and operations will meet that organization's security needs. • Is the desired cloud service FedRAMP- approved, and if so, can the service provider provide a FedRAMP implementation plan? • If the service provider is not FedRAMP-approved, can they supply a security asset and operations implementation plan that has detail similar to that of a FedRAMP implementation plan that can be provided to the Agency? • According to the FedRAMP (or other) implementation plan, how does the commercial service provider's security asset and operations infrastructure compare to that of the Agency's existing and/or desired security infrastructure? • If a gap exists between the desired security posture of the Organization and the controls offered by the CSP, what SLAs can be created to reduce or eliminate the gap? • Even if the service provider's security infrastructure looks to be sufficient on paper, does the Agency have specific high-value assets that require a higher FedRAMP baseline, more security rigor than the service provider is planning to provide, or that should simply not be migrated to the cloud? • To address security gaps between the desired security state and the security state offered by the service provider, what options are available to address those gaps? For example, can additional security services be discussed in the context of a service level agreement or provided by 3rd party cloud services.	
Cloud Guidance	If an Agency is acquiring a FedRAMP-approved commercial cloud service, it is recommended that they request that service's FedRAMP implementation plan, which contains information regarding its security assets and operations. It is recommended that Agencies examine their current on-premise asset and operational setup to compare to the commercial service's implementation to determine if it is sufficient for their purposes, making the assumption that the Agency's current security requirements are	

Area	Analysis
	sufficient. If there are any gaps in asset configurations and/or operations compared to the Agency's desired security level, Agencies can either leverage the SLA process to request the appropriate asset and operational changes, modify their FedRAMP control baseline level, or they can choose to not move certain high-value data and applications to that commercial cloud service. This success of this guidance is based on several assumptions. For example, there is an assumption that the cloud service provider accurately represents their security infrastructure and operations in the FedRAMP implementation guide. In addition, the FedRAMP implementation plan describes the commercial provider's security implementation at a given point in time, which over the course of normal operations, may change. In the case that an Agency is not subscribing to a FedRAMP-approved it is recommended that Agencies request the commercial service provider's security asset and operations FedRAMP implementation plan equivalent to perform a similar analysis as described above.
Applicable FedRAMP Controls	With on premise hardware, agencies have physical visibility and control. With cloud, agencies have contractual control. It is not clear that the latter is "reduced." It should be at least as good: agencies should not be granting ATO to CSOs if the risk is not deemed acceptable. Depending on the agency and CSP involved, it may be enhanced. The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the Physical and Environmental Protection (PE) control family, the System and Communications Protection (SC) control family, and the System and Information Integrity (SI) control family (especially control SI-4 Information System Monitoring)—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). For full information on FedRAMP, go to fedramp.gov.
Supporting Data	These articles provide additional discussion for this cloud security consideration.[158,159]

Malicious Provisioning of Resources

Overview

In a commercial cloud environment, if an attacker, or malicious insider, gains access to an Agency's cloud services, for example through compromised credentials or a compromised API, the attacker could have the ability to provision additional resources that could be used to target external entities as well as internal Agency assets. This situation gives the attacker greater computing capabilities, unlike in a traditional on-premise environment where the computing resources are limited to what is physically on site.

[158] https://arxiv.org/ftp/arxiv/papers/1601/1601.05329.pdf
[159] https://www.itworldcanada.com/blog/is-loss-of-control-the-biggest-hurdle-to-cloud-computing/95131

The malicious provisioning of additional resources may be used to initiate attacks that are focused internally to the Agency as well as attacks that target external entities using compromised assets. Such attacks include distributed denial of service attacks and botnet attacks. The attacker may also change configuration settings to make data publicly available, allow the flow of previously blocked traffic into an Agency's network, and create new user accounts; thus, there is the potential loss of confidentiality, integrity, and/or availability of agency data and resulting impacts on Agency's mission. Additionally, the impact to an Agency may be economically focused, as Agencies are charged for their usage of cloud services, the malicious provisioning of resources has the potential to rapidly drive up Agency costs or increment costs slowly to reduce the chance of detection.

This cloud consideration is impacted by the cloud characteristics: Resource Pooling and Data Replication.

Analysis

<table>
<tr><th>Area</th><th colspan="2">Analysis</th></tr>
<tr><td rowspan="3">Cloud Service Model Considerations</td><td>SaaS</td><td rowspan="2">Provisioning of resources is limited at the SaaS and PaaS levels.</td></tr>
<tr><td>PaaS</td></tr>
<tr><td>IaaS</td><td>Provisioning of resources at the IaaS level is expansive as new networks, virtual machines, private clouds, firewalls, accounts and other resources can be created, modified, or deleted.</td></tr>
<tr><td rowspan="2">Risk Analysis</td><td>Loss of Confidentiality, Integrity, and Availability</td><td>This cloud consideration can lead to the loss of Confidentiality, Integrity and Availability of Agency data depending on the course of action taken by the perpetrator.</td></tr>
<tr><td>Risk to NIST Framework Implementation</td><td>This cloud consideration impacts Identity Management, Authentication and Access Control PR.AC, Data Security PR.DS, Protective Technology PR.PT, Anomalies and Events DE.AE, Security Continuous Monitoring DE.CM, Detection Processes DE.DP, Analysis RS.AN, and Mitigation RS.MI.</td></tr>
<tr><td>Considerations to Guide Recommendations</td><td colspan="2">The following considerations, can enhance an Agency's ability to mitigate an attacker's capacity to provision resources with compromised credentials in commercial cloud environments.
What are the roles and responsibilities of all stakeholders regarding compromised credentials in the cloud?
How do the service providers and consumers define a "compromised credential"?
How can the accounts of compromised users be identified?
How can compromised accounts be isolated and restricted in their ability to provision further resources?
How can resources that have been provisioned by a compromised account be identified and isolated/quarantined?
What tools and policies can be developed or are provided by a CSP to mitigate malicious provisioning or modification of resources?
To what extent can CSP log and monitor all privileged account activities?
Who is responsible for the detection of malicious provisioned resources, and how quickly can they be identified?
What policies does the Agency have in place to limit the ability of privileged accounts such as separation of duties?</td></tr>
<tr><td>Cloud Guidance</td><td colspan="2">A CSA recommendation is that implementers should ensure adequate security zones for different types of machines. Servers, development machines, workstations and management consoles should each have their own security zone. Providers must have</td></tr>
</table>

Area	Analysis
	a reporting mechanism in place that provides evidence of isolation and raises alerts if there is a breach of isolation. It is also possible to enforce NAC137 (Network Access Control)-like capabilities to isolate stale VM's until their rules and pattern files are updated and a scan has been run.[160]
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the Configuration Management (CM) and System and Communications Protection (SC) control families—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	Articles illustrate how cloud resources can be used for malicious (or unintended) purposes.[161,162]

Compromise of Credentials

Overview

Credentials represent the gateway into an organization's data and services, whether they are housed in an on-premise network or in the commercial cloud environment. If credentials are compromised, this represents a significant security consideration for either on premise or commercial cloud environments.

According to the literature, detection of compromised credentials in the cloud is a challenge.[163] If valid Agency cloud credentials are compromised, attackers may leverage valid login mechanisms which will not alert the Agency or the CSP to malicious access to government data. Detection mechanisms to catch the use of compromised credentials could include maintaining a close watch over login behavior, e.g. geolocation enabled IP addresses, temporal login discrepancy, multiple logins, type of device user is logging in from, etc., however, many CSPs have varied and limited log data available via APIs for the Agencies to do this monitoring, even if the Agency had resources to do so. Logs of cloud usage could also indicate that credentials have been compromised if data access activity does not match that of the actual Agency. This approach also assumes that certain log information is made available to the customer organization by the CSP.

Certain commercial cloud characteristics create additional cyber risks related to the compromise of credentials that are unique to the cloud environment as compared to on premise environments. If higher-level authority credentials, such as administrator-level credentials, are compromised, an attacker can create new VMs and can allocate and re-allocate computing resources, create new credentials, dynamically provision new resources in greater amounts than would be possible in an on-premise network, among other actions. Additionally, such a compromise could include changing what alerts would be sent and what data is monitored for alerting.

[160] https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf
[161] https://www.infosecurity-magazine.com/opinions/comment-botnets-the-dark-side-of-cloud-computing/
[162] https://www.wired.com/2014/07/how-hackers-hid-a-money-mining-botnet-in-amazons-cloud/
[163] http://searchcloudsecurity.techtarget.com/news/2240242723/Account-credentials-emerge-as-a-weak-spot-for-cloud-app-security

Please see the considerations "Malicious Provisioning of Resources" and "Increased Opportunity for API Compromise" for additional information on what an attacker can do if they gain access to a commercial cloud service and for recommendations for this occurrence.

This cloud consideration is impacted by the cloud characteristics: Commingling of Data, One-to-Many, and CSP Interdependency.

Analysis

<table>
<tr><th>Area</th><th colspan="2">Analysis</th></tr>
<tr><td rowspan="3">Cloud Service Model Considerations</td><td>SaaS</td><td rowspan="3">Poses no discernable difference in its impact on the cloud service models.</td></tr>
<tr><td>PaaS</td></tr>
<tr><td>IaaS</td></tr>
<tr><td rowspan="2">Risk Analysis</td><td>Loss of Confidentiality, Integrity, and Availability</td><td>This cloud consideration can lead to the loss of Confidentiality, Integrity and Availability of Agency data, particularly if the perpetrator gains access to credentials with greater privileges.</td></tr>
<tr><td>Risk to NIST Framework Implementation</td><td>This cloud consideration impacts Risk Assessment ID.RA, Identity Management, Authentication and Access Control PR.AC, Awareness and Training PR.AT, Data Security PR.DS, Information Protection Processes and Procedures PR.IP, Protective Technology PR.PT, Anomalies and Events DE.AE, Continuous Monitoring DE.CM, Detection Processes DE.DP, Analysis RS.AN, and Mitigation RS.MI.</td></tr>
<tr><td>Considerations to Guide Recommendations</td><td colspan="2">The following questions can guide an Agency's ability to mitigate risks associated with the compromise of their credentials in the commercial cloud.
What types and strengths of authentication are supported by a CSP? For example, is two-factor authentication supported?
What login data, both successful and failed attempts, are tracked by the CSP?
What password policies does the Agency have enforced? Additionally, can the Agency impose a stronger password policy through the CSP?
Is login data available to the Agency via an API or other reporting mechanism?
What policies exist to reduce the number of elevated/privileged access accounts?
What additional login commercial alerting capabilities are available to the customer Agency?
What separation of duties policy exists for Agencies?
What policy is in place for multi-factor authentication?
What capabilities are available to analyze login anomalies?
What administrator actions are logged and analyzed?</td></tr>
</table>

Area	Analysis
Cloud Guidance	Agencies are recommended to leverage robust authentication approaches to mitigate the risk of compromised cloud credentials, such as multi-factor authentication. These strategies apply to usernames, passwords, and private keys.[164] If an Agency wishes to track login activity for potential compromises in credentials, they should request that this monitoring either be done by the CSP and reported to the Agency, or the login data should be make available to the Agency via an API so that the Agency can maintain its own login analysis capability. Separation of resources and duties for an Agency's commercial cloud service is recommended. For example, it is not recommended that Agencies leverage a single API key to access and to run all cloud functions. Responsibilities, and therefore credentials, should be broken up such that a single credential compromise cannot make an entire Agency's data vulnerable. This strategy does not prevent this attack, but it can limit the exposure of data and applications should this attack occur.
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the Access Control (AC), Identification and Authentication (IA), and Incident Response (IR) control families—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	Additional resources highlighting the nature of this cloud security considerations, the impacts and possible mitigations.[165,166,167,168]

Increased Attack Surface due to Multi-Tenancy

Overview

Multi-tenancy of commercial cloud hardware can increase the attack surface in this computing environment, leading to a variety of issues that have impacts on .gov data security. System and software vulnerabilities within a CSP's infrastructure, platforms, or applications that support multi-tenancy can lead to isolation failure in the case that an attacker exploits the vulnerability to access another tenant's assets/data.[169] This can be accomplished through exploiting vulnerabilities in the applications or hypervisor, subverting logical isolation controls, or attacks on the management API.

On type of vulnerability is VM escape. This occurs when a hacker intentionally breaks out of a Virtual Machine (VM) to gain host access, subsequently gaining access to other hosted VMs and to the host

[164] http://searchcloudsecurity.techtarget.com/answer/Cloud-authentication-Whats-the-best-way-to-secure-cloud-credentials
[165] https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf
[166] https://www.infosecurity-magazine.com/opinions/employees-compromised-credentials/
[167] https://www.networkworld.com/article/3056823/security/a-new-approach-to-detecting-compromised-credentials-in-real-time.html
[168] https://www.csoonline.com/article/3022066/security/60-of-companies-cannot-detect-compromised-credentials-say-security-pros-surveyed.html
[169] Threats and Risks Faced by Agencies Moving to the Cloud (DHS CS&C March 2017)

operating environment. This attack has been demonstrated in research settings and has been reported as a known vulnerability for VMs.[170,171]

While companies in a traditional on-premise environment may host servers on VMs locally, in the cloud, the use of VMs, rather than operating systems running on "bare metal," are practically guaranteed. VM misconfiguration or successful exploit of a vulnerability in a VM can lead to VM escape and subsequent potential compromise of the other tenants on that VM. The impacts of VM escape can be devastating as the perpetrators are able to monitor traffic, exfiltrate data, create accounts, etc., as they gain access to many different levels of the services with little in the way to contain them. Verifying and validating images, patching networks and systems, encryption and key management, and building in security controls, such as VM introspection, within the virtual environment that can detect and prevent unauthorized activities should be requirements for managing VMs.

This cloud consideration is impacted by all of the cloud characteristics previously introduced.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS* *PaaS* *IaaS*	All models are affected since the cloud in general uses virtualiation as a foundation for services (backend). However, IaaS is more likely to be affected for two reasons: 1. In IaaS tenants will create many VMs to meet their business needs, and 2. Most interaction with PaaS and SaaS are done using application interfaces and/or APIs, which do not have the ability to communicate directly with a VM (frontend).
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	This cloud consideration can impact the confidentiality, integrity and availability of Agency data depending on the type of attack.
	Risk to NIST Framework Implementation	This cloud consideration will impact Risk Assessment ID.RA, Risk Management Strategy ID.RM, Identity Management, Authentication and Access Control PR.AC, Data Security PR.DS, Information Protection, Processes and Procedures PR.IP, Protective Technology PR.PT, Anomalies and Events DE.AE, Security Continuous Monitoring DE.CM, Detection Processes DE.DP, Communications RS.CO, and Analysis RS.AN.
Considerations to Guide Recommendations	The following questions can enhance an Agency's ability to mitigate risks associated with the increased attack surface due to multi-tenancy. • What isolation controls, if any, are offered by the CSP? • What security options can the CSP provide in the way of verifying and validating images? • What detection tools has the CSP deployed for identifying and containing unauthorized access and use of VMs? • How does the CSP identify an incident of VM Escape in the cloud and what VM escape detection capabilities are deployed by the CSP? • Will tenants/customers be informed if their data or infrastructure is affected by a known VM escape event? Will tenants/customers be informed if VM escape affects tenants on	

[170] https://www.darkreading.com/risk/hacking-tool-lets-a-vm-break-out-and-attack-its-host/d/d-id/1131254?
[171] https://nvd.nist.gov/vuln/detail/CVE-2009-1244

Area	Analysis
	hardware shared with the customer, even if the event does not directly affect their data? • What measures has the CSP employed in the way of data loss protection, data encryption, and data recovery? • What configuration management/patching process does the CSP have to patch/update hypervisor vulnerabilities? • What other defenses are in place to mitigate potential compromises, e.g. encryption of data?
Cloud Guidance	NIST 800-144 (Software isolation): Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.[172] VM escape is a challenging consideration to address. For Agencies using a commercial cloud service, it is recommended that Agencies follow best cybersecurity practices for encrypting their data, using their own keys and key management strategies where possible. In IaaS environments, it is recommended that Agencies leverage standard encryption approaches as described in FIPS.[173] Agencies may need to rely on CSPs to detect a VM escape event and to notify them that their data may have been affected. Segmentation should be available at all layers for a secure multi-tenant environment. Especially in the case of IaaS, the Agency should know what isolation provisions are available. Some of the capabilities that are needed include VM segmentation and VM introspection.[174]
Applicable FedRAMP Controls	Agencies are responsible for determining acceptable risk. If an agency deems the risk of multi-tenancy with non-government users for a given computing need unacceptable, then the agency should consider multi-tenancy with government only users. If the agency deems the risk of that unacceptable, the agency should consider an agency-only cloud. Due diligence requires research on the part of the agency to determine the risk involved. Agencies could benefit from assistance here by agencies such as DHS to determine with more precision what the risk due to multi-tenancy is. For full information on FedRAMP, go to fedramp.gov.
Supporting Data	NIST 800-144 Section 4.6 Software Isolation, sub bullet Attack Vectors contains several examples of possible attack vectors.[175] Additional articles highlighting examples of VM escape.[176,177]

[172] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
[173] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
[174] http://searchcloudsecurity.techtarget.com/tip/Securing-a-multi-tenant-environment
[175] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
[176] https://www.pcworld.com/article/3182816/security/pwn2own-hacking-contest-ends-with-two-virtual-machine-escapes.html
[177] https://arstechnica.com/information-technology/2015/05/extremely-serious-virtual-machine-bug-threatens-cloud-providers-everywhere/

Area	Analysis
	"Security in the cloud: The threat of coexist with an unknown tenant on a public environment."[178]

Memory Leakage in Shared Infrastructure

Overview

One type of data leak occurs when a computer incorrectly manages memory, failing to release discarded memory resources from processes that do not require them at a given moment in time.[179] For on premise systems, memory leakage is typically considered a system performance challenge. For example, if memory is not allocated and reallocated correctly, it generates computing inefficiencies as not all memory is available to the user. In extreme cases, unallocated memory can accumulate, causing a computer system to crash, and memory resources become unavailable.[180] Simulation experiments have shown that this phenomenon is possible in a public cloud environment (i.e., accumulation of "orphaned VMs"), potentially affecting data availability for Agencies.[181]

In a shared infrastructure environment, such as a multi-tenant commercial cloud, data leakage can transition from being a computing performance challenge to a security challenge. It is possible to recover sensitive data written by a previous user, such as an Agency, from shared memory after that memory is no longer used by the Agency if the data has not been effectively sanitized before reallocation. Virtual machine replication, or cloning, can lead to another type of data leakage problem regarding machine secrets, such as the exposure of host keys for memory or storage resources. Furthermore, when a cloud provider physically disposes of hardware, the sanitation process is out of the control of cloud tenants. Sensitive Agency data remnants can be recovered by an attacker in this scenario, representing a loss of data confidentiality. NIST 800-144 references examples of these issues.[182,183]

This cloud consideration is impacted by the cloud characteristics: CSP Interdependency and Data Distribution.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS*	Poses no discernable difference in its impact on the cloud service models.
	PaaS	
	IaaS	
Risk Analysis	*Loss of Confidentiality, Integrity, and*	Agencies may not be able to verify that their data was securely deleted from used memory resources that are being reallocated to other users. Data remnants from used memory that have not been

[178] https://pdfs.semanticscholar.org/6e07/c49bfcfbeb23d212669368bc599159d07fcb.pdf
[179] https://www.nist.gov/sites/default/files/documents/itl/antd/VM-LeakageV.pdf
[180] Ibid.
[181] Ibid.
[182] Valli, Craig. "Andrew Woodward, The 2008 Australian Study of Remnant Data Contained on 2 nd Hand Hard Disks: The Saga Continues." *The 6 th Australian Digital Forensics Conference, Perth, Western Australia*. 2008.

[183] Sobey, Charles H., Laslo Orto, and Glenn Sakaguchi. "Drive-independent data recovery: the current state-of-the-art." *IEEE transactions on Magnetics* 42.2 (2006): 188-193.

Area	Analysis	
	Availability	effectively sanitized can become available to attackers. Thus, there is a potential loss of data confidentiality.[184]
	Risk to NIST Framework Implementation	Data leakage in shared infrastructure impacts Access Controls PR.AC, Data Security PR.DS, and Information Protection Processes and Procedures PR.IP.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to appropriately mitigate memory leakage in shared infrastructure: • What types of memory and storage media are housing the data? These factors will have implications for the sanitization method. • Will the Agency be required to verify that their data has been deleted from shared memory infrastructure? If so, how will the Agency work with the CSP to track the location of their data throughout its lifecycle? • What are a CSPs baseline methods for memory sanitization once it is no longer allocated to a user, prior to its allocation to a new user, both in volatile and non-volatile memory. • Given data sensitivity, can an Agency assume that their data has not been adequately deleted from share memory infrastructure and rely on access control mitigations to prevent confidentiality loss?	
Cloud Guidance	Memory is considered a form of electronic media, and therefore all of the guidance included for "Inability to Verify Data Deletion" is applicable to addressing memory leakage in shared environments.[185] Please refer to the "Inability to Verify Data Deletion" for a complete set of data sanitization recommendations. Additional capabilities to mitigate this cloud security consideration include data sanitization, encryption and key management, traffic monitoring and analysis, provisioning controls, authentication and credentialing, and intrusion detection.[186]	
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the implementation and assessment of the controls in the Media Protection (MP) control family (especially MP-6 Media Sanitization) and the System and Communications Protection (SC) (especially SC-7 Boundary Protection) control family—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). For full information on FedRAMP, go to fedramp.gov.	
Supporting Data	"Dropbox analysis: Data remnants on user machines"[187] "Experimental Proof: Data Remanence in Cloud VMs"[188] Survey on Data Remanence in Cloud Computing Environment"[189]	

[184] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
[185] Ibid.
[186] https://www.cloudcomputing-news.net/news/2012/nov/14/preventing-data-leakage-proactive-security-from-the-cloud/
[187] http://www.sciencedirect.com/science/article/pii/S174228761300011X
[188] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7214152

Area	Analysis
	Additional discussion and resources for this cloud security consideration.[190,191,192]

Reduced Capability to Perform Post-Event Forensics

Overview

As part of any cybersecurity incident response effort, the goal of digital forensics is to: (1) discern what happened, (2) understand what portions of the system were affected, (3) learn how to prevent such incidents from happening again, and (4) collect information for possible future legal actions.

In a commercial cloud environment, the Agency no longer owns the hardware and infrastructure that houses its data. Commercial CSPs will not be willing to allow customers/tenants to perform forensics on shared hardware and software involved in an attack, as this could affect the security and/or privacy of other tenants using shared cloud resources. This will lead to reduced capability for an Agency to characterize the nature, origin, intent, and reach of malicious incidents, thus, limiting their ability to respond, recover and incorporate lessons learned in the future. Agencies will need to engage with CSPs in order to decide on the roles and responsibilities for incident response and post-event forensics, including what information will be shared, in what timeframe, and a process through which the Agency can request additional pieces of information. Additionally, if the Agencies need to use this information for legal purposes, the handling and collection of this data must adhere to appropriate forensics and legal standards.

This cloud consideration is impacted by the cloud characteristics: Distribution of Data, CSP Interdependency, One-to-Many, and Adaptable to Multiple CSPs.

Analysis

Area		Analysis
Cloud Service Model Considerations	*SaaS*	It is unknown whether a CSP will allow for any forensics on their hardware.
	PaaS	It is unknown whether a CSP will allow for any forensics on their hardware.
	IaaS	Some forensics can be performed on memory or disks of IaaS assets. However, like SaaS and PaaS, it's very unlikely a CSP will allow for any forensics on their hardware.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	This cloud consideration can lead to loss of the availability, confidentiality, and integrity of Agency data.
	Risk to NIST	This cloud consideration may impact Governance ID.GV,

189 https://www.researchgate.net/publication/317244855_Survey_on_data_remanence_in_Cloud_Computing_environment

190 https://docs.openstack.org/security-guide/tenant-data/data-privacy-concerns.html

191 http://resources.infosecinstitute.com/data-sanitization-for-cloud-storage/

192 https://books.google.com/books?id=FUSnBQAAQBAJ&pg=PA4&lpg=PA4&dq=memory+remanence+cloud&source=bl&ots=D0_wsPVsJe&sig=VhL8wUW_8oXROpj1Suc1M0IVta8&hl=en&sa=X&ved=0ahUKEwiqoNvJw7PZAhXK44MKHetdAWAQ6AEISzAG#v=onepage&q=memory%20remanence%20cloud&f=false

Area	Analysis	
	Framework Implementation	Protective Technology PR.PT, Communication RS.CO, Analysis RS.AN, Mitigation RS.MI, and Improvements RS.IM.
Considerations to Guide Recommendations	The following considerations, adapted from NIST 800-146, can enhance the ability to perform post-event forensics in commercial cloud environments when Agency data is impacted or is suspected to be impacted. • What are the roles and responsibilities of all stakeholders regarding post-event forensics in the cloud? • How do the service providers and consumers define an "incident?" • What is the definition of "cybersecurity incident post event forensics" in the commercial cloud? • How does an Agency integrate with current federal cybersecurity guidelines and relevant CONOPs? o Guidelines for incident handling roles and responsibility definitions in service agreements o Guidelines for clock synchronization across data centers to help reconstruct a chain of events o Guidelines for how data breach notification laws are handled in different countries • What data can a cloud provider access when capturing an image of a shared hard drive and how is this process completed? • What is available to the consumer in an audit log? (e.g., is information related to other cloud consumers protected?) • What is the responsibility of a consumer to report an incident? • Can a cloud service provider legally intervene in stopping an attack on an application in its cloud if it is only an indirect contractual relationship (e.g., three tiers of customers)? • How are post-event forensics roles, responsibilities, and CONOPs streamlined across a diverse population of CSPs? • What jurisdictions must be considered when trying to perform cloud forensics? • What SLAs can be made so that the CSP will aid the Agency in performing forensics? What gaps are left from the traditional methods an Agency would perform forensics with what they will get from a CSP? • How long does the CSP retain logs, data, backups or other artifacts that would be useful to perform forensics?	
Cloud Guidance	NIST SP800-146 states that: *Forensic analysis in a SaaS model may be the sole responsibility of a provider while forensic analysis in an IaaS model may be the primary responsibility of the consumer (with some collaboration with the provider). The PaaS model appears to split responsibilities between consumers and providers.*[193] Post-event forensics is primarily the responsibility of the Agency, it is recommended that Agencies establish the roles and responsibilities for completing post-event forensics in the cloud, which may depend on what service model is being leveraged. It is recommended that Agencies establish clear expectations of the content of any forensic analyses to be performed by the CSP on behalf of the Agency.	

[193] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

Area	Analysis
	Agencies can refer to Administrative memorandum *OMB-M-07-16* as well the additionally cited sources for specific guidance on their requirements regarding a data breach to inform SLA language with a CSP with regards to roles and responsibilities pertaining to post-event forensics.[194][195,196]
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the implementation and assessment of the controls in the Incident Response (IR) control family—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	These articles feature discussion for this cloud security consideration, including overview, challenges and legal issues.[197,198,199,200] "Time synchronization: pivotal element in cloud forensics."[201]

Latency-Induced Loss of Situational Awareness

Overview

An Agency's ability to maintain situational awareness depends, in part, on how quickly data and network activity logs are available for analysis. Changes in an Agency's computing environment, such as a transition to a commercial cloud service provider, may introduce latencies in acquiring activity logs due to the reliance on the CSP to make these logs available to the Agency for analysis. Latency in log acquisition can lead to loss of situational awareness, and increase an Agency's difficulty to perform real-time monitoring of an attack.

NIST SP 800-146 defines latency as:

> Latency is the time delay that a system experiences when processing a request. Latency experienced by cloud consumers typically includes at least one Internet round-trip time, i.e., the time it takes for a request message to travel to a provider plus the time it takes for the response message to be received by a consumer. Generally, Internet round-trip times are not a single expected number but instead a range, with a significant amount of variability caused by congestion, configuration error, or failures. These factors are often not under the control of a provider or consumer.

[194] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf
[195] https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf
[196] https://link.springer.com/chapter/10.1007%2F978-3-319-67208-3_7
[197] http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf
[198] https://arxiv.org/ftp/arxiv/papers/1410/1410.2123.pdf
[199] http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-forensics-challenges
[200] https://www.forensicmag.com/article/2015/05/legal-issues-cloud-forensics
[201] http://onlinelibrary.wiley.com/doi/10.1002/sec.1056/full

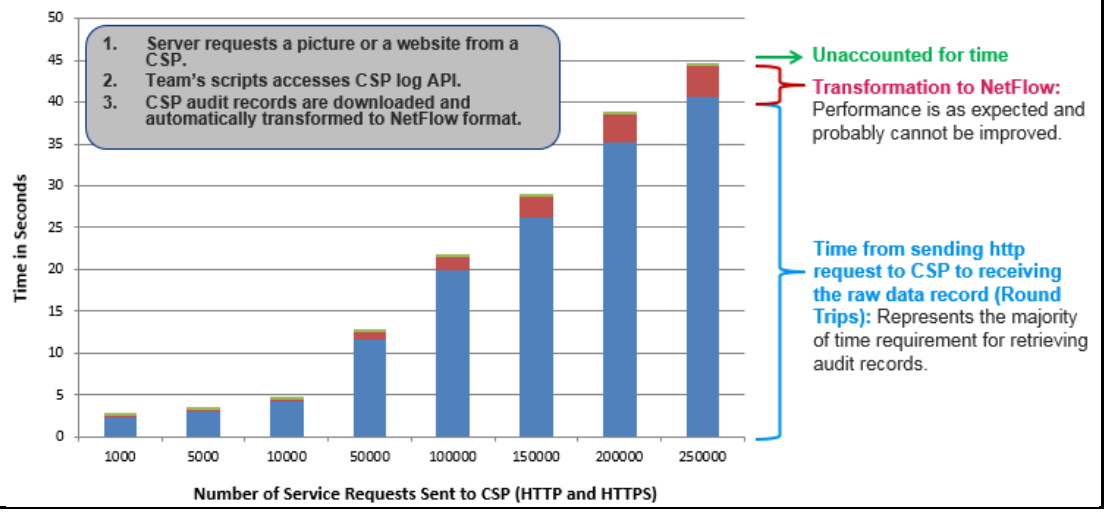
In an on-premise network environment, monitoring of network traffic can be done in near real-time since the Agency owns and operates the networks and nodes the data is traversing. In the cloud, the agency doesn't necessarily have real-time access and does not own the equipment or networks since they are tenants, introducing logistical and location-derived delays in obtaining log data, even without CSP log data processing times.

Additional cloud characteristics can amplify this latency. For example, in the case of CSP interdependency, a CSP may be relying on a third party CSP to do Agency data processing. If logs are generated from the third-party processing of Agency data, it may require additional time for the primary CSP to assimilate and to make available these logs for situational awareness of the Agency.

This cloud consideration is impacted by the cloud characteristics: CSP Interdependency and Distribution of Data, One-to-Many and Adaptable to Multiple CSPs.

Analysis

<table>
<tr><th>Area</th><th colspan="2">Analysis</th></tr>
<tr><td rowspan="3">Cloud</td><td>SaaS</td><td rowspan="3">Latencies may vary between CSPs and additionally CSPs may offer additional services to mitigate latency; thus, the impact on the service models will depend highly on the CSP.</td></tr>
<tr><td>PaaS</td></tr>
<tr><td>IaaS</td></tr>
<tr><td rowspan="2">Risk Analysis</td><td>Loss of Confidentiality, Integrity, and Availability</td><td>Latencies in acquiring logs can result in the loss of data confidentiality, integrity, and availability.</td></tr>
<tr><td>Risk to NIST Framework Implementation</td><td>Latency-Induced Loss of Situational Awareness may impact Anomalies and Events DE.AE, Security Continuous Monitoring DE.CM, Detection Processes DE.DP, Communications RS.CO, Analysis RS.AN, and Mitigations RS.MI.</td></tr>
<tr><td>Considerations to Guide Recommendations</td><td colspan="2">The following questions can guide an Agency’s ability to anticipate loss of situational awareness due to latency in acquiring log data in the commercial cloud service.
What logs are available to an Agency from the service provider for the specific service planned to be leveraged, either from APIs or via other reporting mechanisms?
When performing test operations with a new commercial service prior to transitioning actual Agency resources to a new cloud service, what is the time period between performing an operation until the associated log information is made available by the CSP? How does this time lag compare to that of the Agency’s current network?
Is the increase in time lag between an operation occurring and the log data availability acceptable in the new cloud environment?
Are some Agency assets high value enough to warrant needing faster log availability times?
What 3rd party options may be available such as a CASB that could help in monitoring traffic and providing near-real time protections?</td></tr>
<tr><td>Cloud Guidance</td><td colspan="2">Some Agencies may be able to adapt to the latency in log availability and the resulting changes in situational awareness and ability to detect cyber-attacks due to the nature of their data. For example, some Agencies may have data that is less sensitive compared to others, and therefore maintaining situational awareness is not as urgent compared to Agencies handling more sensitive data types. Agencies that expect situational awareness to be impacted due to transition to a CSP are recommended to communicate to their stakeholders the expectation that situational awareness may be delayed due to their transition to cloud services.</td></tr>
<tr><td>Applicable FedRAMP Controls</td><td colspan="2">The System Security Plan (SSP) for a CSO describes the CSP’s implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that</td></tr>
</table>

Area	Analysis
	implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the implementation and assessment of the controls in the Audit and Accountability (AU) control family (especially control AU-7 Audit Reduction and Report Generation), the System and Information Integrity (SI) control family (especially control SI-4 Information System Monitoring), and the Incident Response (IR) control family—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	Article on latency in the cloud in general.[202] CSP provides information on event payload, timeliness and delivery frequency.[203] DHS previously performed log acquisition testing at a variety of commercial CSPs. Among other measurements, DHS captured timestamps of cloud service requests and resulting CSP log availability to capture the time duration between these events. As an example, requesting and waiting for audit records from one CSP via their commercial APIs represented the majority of the time requirement for this duration. As cloud service requests increased in frequency, so did the latency between the service request and the log availability. Please see the below figure for a graphical representation of these findings. 

Reduced Ability to Secure Unknown Agency Cloud Workloads

Overview

For information security reasons, an Agency's IT staff may maintain its own data monitoring toolset to meet its unique data security needs given its mission and the types of data it handles. In order to maintain security coverage over all of an Agency's assets, its IT support needs to be aware of all of the computing activities being performed by the Agency workforce.

As an Agency transitions to a commercial cloud environment, although monitoring strategies may change to accommodate a new computing environment, IT support must maintain knowledge of the Agency's

[202] https://www.interxion.com/globalassets/_documents/whitepapers-and-pdfs/cloud/WP_TRUTHANDLIES_en_0715.pdf
[203] https://aws.amazon.com/cloudtrail/faqs/

computing activity and assets in order to successfully accomplish any information security responsibilities it maintains.

For both on-premise traditional and commercial cloud environments, Agency workforce members may access or provision resources that the Agency's IT staff is not aware of. For example, two Agency workforce members may try to share a large document that won't transfer via email, and decide to use a CSP's data storage and file sharing service to do the file transfer instead. The employees do not inform IT support that they are using cloud services to handle Agency data, thus the transfer is not monitored.

If Agency personnel are using cloud assets to do their work without the agency's IT staff being aware of it, these workloads might not be sufficiently protected. IT staff are not able to manage, log and monitor these unknown cloud workloads or other shadow IT. For IaaS instances, personnel can create new VMs or other instances without IT support knowledge, which may lead to instances that are not monitored for security purposes. Unknown workloads could be a policy violation as well is agency members of the workforce use cloud resources that are not in their agency's service contract or are not authorized by the Agency that could potentially violate policies such as ITAR, HIPAA, etc.

This cloud consideration is impacted by the cloud characteristic Distribution of Data.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS*	SaaS workloads are limited to the type of software application used and represents the smallest potential for unknown agency workloads compared to other service models. However, these types of services can be the easiest for Agency users to setup and use outside of traditional IT.
	PaaS	Workloads on PaaS are limited to the platform(s) used by the Agency and represent a smaller potential for unknown agency workloads compared to IaaS, but represent a greater potential for this consideration compared to SaaS.
	IaaS	IaaS represents the greatest potential for unknown agency workloads due to the number of types of workloads that can be created and used by a user.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	Processing, storing or transferring Agency data through CSP services without proper authorization, Agency knowledge, etc. can lead to a loss of Confidentiality and Integrity or Agency data if the data is compromised.
	Risk to NIST Framework Implementation	This cloud consideration impacts Asset Management ID.AM, Governance ID.GV, Risk Management Strategy ID.RM, Identity Management, Authentication, and Access Control PR.AC, Awareness and Training PR.AT, and Data Security PR.DS.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to address the challenge of unknown agency workloads. • Do the Agency workforce members understand what services and instances they are allowed to create in their commercial cloud instance? What types of awareness and education can be leveraged to raise awareness at the Agency regarding what types of workloads they are authorized to create? • Is there a mechanism for Agency workforce members to leverage if they need additional cloud resources so that they may be	

Area	Analysis
	created appropriately and securely? • Is a commercial service, such as a commercial access security broker (CASB) or service such as Amazon Cloudwatch, configured to monitor agency cloud activity that could potentially detect unknown workloads? • Are the Agency's accesses configured such that the members of the workforce have the appropriate privileges? • What monitoring capabilities does the Agency have to detect employees using non-approved CSP offerings?
Cloud Guidance	The following recommendations can help Agencies address unknown cloud workloads: **Monitoring**: Leverage CASBs and services such as Amazon Web Service's CloudWatch can be configured to monitor instances for changes or modifications to alert IT support that a change is being made. **Education & Awareness**: Training programs and awareness among members of the workforce to avoid unknown workloads. Also, make needed cloud resources available so the unknown workloads are not needed. **Set Workload Privileges**: Assign privileges appropriately among members of the workforce so that folks that have taken training and have awareness of approved workloads can provision new ones.
Applicable FedRAMP Controls	Agencies should have policies in place as part of the agencies' Rules of Behavior (see control PL-4 Rules of Behavior) prohibiting the use of unapproved cloud usage. This is not an issue that FedRAMP can address. (See the FedRAMP Cloud Memo.)
Supporting Data	Additional articles discussing Shadow IT in the cloud, the issues, the impacts and mitigations.[204,205,206,207]

Web-based Attacks

Overview

Web-based attacks can occur in traditional on premise and commercial cloud environments. Examples of current web-based attacks include attacks on web-based applications, APIs, and include cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, script injection, replay attacks, and others.[208] In on premise networks, these attacks can occur as users behind the perimeter leverage web browsers or APIs, and for cloud environments, these same attacks are relevant as cloud users leverage web interfaces and APIs.

[204] https://www.symantec.com/content/en/us/enterprise/other_resources/b-enterprise-security-in-the-cloud.en-us.pdf
[205] https://www.ibm.com/information-technology/how-overcome-cloud-services-challenge-shadow-it
[206] https://www.networkworld.com/article/2997152/cloud-computing/five-ways-shadow-it-in-the-cloud-hurts-your-enterprise.html
[207] https://www.skyhighnetworks.com/cloud-security-university/what-is-shadow-it/
[208] https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

In observed commercial cloud environments, APIs are heavily leveraged for operations such as collecting log and other monitoring data as well as for accessing general cloud functionality. Since APIs are so heavily leveraged, they have the potential to be an attractive target for web-based malicious activity.

These attacks can occur via a web browser, communications to the cloud, web servers (within the cloud) and leverage a variety of avenues for ingress including unpatched (un)known vulnerabilities in web-associated infrastructure.

Some specific examples include vulnerabilities in protocol implementations that create avenues for session tapping and/or hijacking. Internet protocol vulnerabilities that allow man-in-the-middle attacks are also relevant to cloud environments. Browser isolation vulnerabilities might allow third party content to manipulate a web application administered by either an Agency in a IaaS or PaaS service instance, or administered by the CSP in the case of SaaS.

This cloud consideration is impacted by the cloud characteristics: CSP Interdependency, Distribution of Data, and Adaptable to a Diversity of CSPs.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS*	Web-based attacks can occur in SaaS service instances. For SaaS service models, an Agency has no control over the security of the web-based software/application they are consuming from the CSP and are reliant upon the CSP for proper security against these attacks. It should be noted that this responsibility model applies only when the Agency user is using a SaaS service that has been developed and supplied by the CSP and not to a SaaS service that the Agency user has developed themselves on top of a PaaS or IaaS platform provided by the CSP. The latter example of an Agency developing and using a SaaS instance on top of a CSP platform is considered to be a PaaS or IaaS service model consideration in this analysis.
	PaaS	Web-based attacks can occur in PaaS service instances. The PaaS model has a shared responsibility model between the CSP and the end user that is developing applications on top of CSP-provided infrastructure, each owning respective responsibility against web-based attacks on the instances they have developed themselves. Depending on the platform used by the Agency, the Agency must consider risks to that application they are creating and hosting on the platform they are using. If a user is leveraging an existing API to write their own application, then there is shared responsibility: CSP owns responsibility for the existing API, but all instances in front of that API is the user's responsibility since the user developed it.
	IaaS	Web-based attacks can occur in IaaS service instances. Agencies leveraging web applications and associated infrastructure on their own IaaS instances bear the full responsibility of web-based attacks.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	Web-based Attacks can lead to a loss of the confidentiality, integrity and availability of Agency data.
	Risk to NIST Framework	Web-based Attacks may impact Risk Assessment ID.RA, Risk Management Strategy ID.RM, Identity Management,

Area	Analysis	
	Implementation	Authentication and Access Control PR.AC, Data Security PR.DS, Information Protection, Processes and Procedures PR.IP, Protective Technology PR.PT, Anomalies and Events DE.AE, Security Continuous Monitoring DE.CM, Detection Processes DE.DP, Communications RS.CO, and Analysis RS.AN.
Considerations to Guide Recommendations	The following questions can enhance an Agency's ability to address the challenges of an Web-based Attack. • How do the service providers and consumers define an "incident" or "Attack" in the cloud? • What are the roles and responsibilities of stakeholders regarding the disclosure of information pertaining to Web-based attacks in the cloud? • Through what channels will an Agency be notified that a Web-based attack may have taken place against the CSP? Will they only be notified if Agency data/services are impacted? • How can Agencies assess the ability of the CSP to detect, respond to, and recover from Web-based attacks? • What security measures are employed by the CSP regarding data loss prevention and data security to limit the long-term impacts of a Web-based attack? • Does the CSP offer perimeter firewalling, segmentation, encryption and/or other tools to protect Agency assets? • What tools does the CSP possess to characterize a Web-based attack and improve their defenses to protect against such incidents in the future? • What training is available to Agency staff and administrators to educate them on steps they can take to minimize vulnerabilities to these threats on the user end?	
Cloud Guidance	For Agencies leveraging CSP-developed and provided SaaS web applications, while the Agency is not responsible for protecting that infrastructure, it is recommended that an Agency ask to be informed if the CSP has knowledge that a web-based attack has occurred that potentially affected its data, or that of another tenant that the Agency shares cloud resources within a multi-tenancy environment. For Agencies leveraging PaaS or IaaS web applications and processes that they have developed themselves, it is recommended that Agencies leverage testing of this infrastructure, perform ongoing vulnerability discovery and patching, and perform ongoing monitoring for detection of these attacks. **Testing**: Prior to using a newly developed web application in either a PaaS or IaaS environment with Agency data, it is recommended that Agencies perform integration testing and penetration testing (aka red-teaming) on their developed APIs for web-based attack vulnerabilities in addition to the typical functionality and scalability testing that an Agency might already perform. Ideally, security testing involves the Agency acting as a faux adversary to find API errors and/or vulnerabilities before Agency data is processed. APIs are heavily relied upon in cloud environments for logging, creating data, deleting data, accessing data, etc, so they will be an attractive target for attackers. A good starting point for penetration testing is to pretend to attack the API with any of the top 10 OWASP attacks to check for known vulnerabilities as	

Area	Analysis
	this may represent a typical starting point for an adversary.[209] Evaluating an API's security against these attacks represents a basic starting point for vulnerability testing. In general, it is recommended that Agencies test for web-based vulnerabilities in their PaaS and IaaS web applications the same way that they would go about this process for an on premise traditional network. For some detail on testing for some of these vulnerabilities, please see the following resources: • https://www.veracode.com/cross-site-scripting-vulnerability; • http://ieeexplore.ieee.org/document/7867260/ • https://www.digitalocean.com/community/tutorials/how-to-secure-a-cloud-server-against-sql-injection **Addressing vulnerabilities**: It is recommended that web-based vulnerabilities are tracked and that available vulnerability patches and updates are promptly performed, just as an organization would normally perform for an on-premise network. **Detection**: It is recommended that, similarly to on premise networks, an Agency monitor for web-based attacks via any log, or other, monitoring data they gather from their cloud instances.
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the implementation and assessment of the controls in the Audit and Accountability (AU) and the System and Communications Protection (SC) control families (especially control SC-7 Boundary Protection)—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	XSS attack on a SaaS CSP discovered, August 2015.[210] Additional articles discussing this cloud security consideration.[211,212,213,214,215]

Advanced Persistent Threat

Overview

NIST SP 800-39 defines the advanced persistent threat (APT) as follows:

[209] https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
[210] https://www.symantec.com/connect/blogs/salesforce-accounts-susceptible-hijacking-using-xss-flaw
[211] https://www.scmagazineuk.com/web-application-attacks-accounted-for-73-of-all-incidents-says-report/article/682004/
[212] http://searchcloudsecurity.techtarget.com/tip/Why-web-application-attacks-are-a-growing-threat-to-the-cloud
[213] https://www.infosecurity-magazine.com/news/web-application-attacks-ansomware/
[214] http://www.computerweekly.com/news/2240219265/Cyber-attacks-move-to-cloud-with-adoption-report-shows
[215] https://www.csoonline.com/article/2991409/cloud-security/application-attacks-against-clouds-up-45.html

> An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.[216]

APTs are a concern in the commercial cloud environment, residing as #7 of the Cloud Security Alliance's 2016 Treacherous 12 Cloud Computing Top Threats.[217] These threats may be tailored made to reach a specific target through multiple avenues, in which case common security measures may not detect any anomalous behaviors. An APT may establish a foothold within a cloud system for the purpose of observing how the system behaves, data flows, user behavior, and other forms of reconnaisance over an extended period of time while also slowly exfiltrating small pieces of data. These types of attack may expand in scope and nature during their duration and can lead to severe impacts for the CSP and the Agency. Agencies should assume a malicious actor will gain access to their data, applications and services and thus take appropriate defense-in-depth approach to their security. Agencies will need to engage with CSPs to enable firewalls, segmentation, encryption, monitoring, and detection capabilities to better protect their assets in the cloud as well as coordinate incident response activities for quarantine, clean-up, configuration changes, forensics, etc.

This cloud consideration is impacted by the cloud characteristics: CSP Interdependency, Distribution of Data, Adaptable to a Diversity of CSPs, One-to-Many, and Many-to-One.

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS*	APTs are applicable to SaaS and PaaS service models. For SaaS and PaaS instances, it is the responsibility of the CSP to monitor for potential APT activity within their environment. Due to redundancies in data and services typically performed by a CSP, if servers are taken down to stop and to clean up an APT, a customer may not even know that there was an attack due to a lack of service interruption, however interruptions in service are a potential outcome of this consideration.
	PaaS	
	IaaS	APTs are applicable to IaaS service models. Agencies may be more heavily relied upon for detection of such evens if they affect the Agency's data. In the case of IaaS, the CSP may or may not even be monitoring for the same malicious activities present on SaaS instances.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	The outcomes of an APT attack in the cloud may lead to a loss of confidentiality, integrity and availability of Agency data.
	Risk to NIST	The APT attack may impact Risk Assessment ID.RA, Risk

[216] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
[217] https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

Area	Analysis	
	Framework Implementation	Management Strategy ID.RM, Identity Management, Authentication and Access Control PR.AC, Data Security PR.DS, Information Protection, Processes and Procedures PR.IP, Protective Technology PR.PT, Anomalies and Events DE.AE, Security Continuous Monitoring DE.CM, Detection Processes DE.DP, Communications RS.CO, and Analysis RS.AN.
Considerations to Guide Recommendations	The following questions can enhance an Agency's ability to address the challenge of an APT. • How do the service providers and consumers define an APT attack in the cloud? • What are the roles and responsibilities of stakeholders regarding the disclosure of information pertaining to APT attack in the cloud? • Through what channels will an Agency be notified that an APT attack may have taken place against the CSP? Will they only be notified if Agency data/services are impacted? • What monitoring and dection capabilities does the CSP provide to discover APTs? • How can Agencies assess the ability of the CSP to detect, respond to, and recover from an APT attack? • What security measures are employed by the CSP regarding data loss prevention and data security to limit the long-term impacts of an APT attack? • Does the CSP offer perimeter firewalling, segmentation, encryption and/or other tools to protect Agency assets? • What tools does the CSP possess to attribute a set of attacks to the same APT source? Is the CSP able to inform an Agency as to which events are attributed to which source? • What training is available to Agency staff and administrators to educate them on steps they can take to recognize (spear) phishing attempts and minimize vulnerabilities to these threats on the user end?	
Cloud Guidance	Recommended guidance to Agencies to help address the challenge of APTs in the commercial cloud is similar to what would be recommended to address this consideration in a traditional on premise network, since an APT is likely to enter a cloud instance the same way that it would gain access to an on premise network. A typical APT strategy involves a combination of educating users, testing developed computing resources, and monitoring for potential APTs. Detection and notification responsibilities become distributed among stakeholders in a cloud environment, depending on the service model in use. **Education**: APTs can establish themselves through a variety of vectors including phishing, spear phishing, unknown or unpatched vulnerabilities, etc. It is recommended that, similar to an on premise network scenario, Agencies educate their cloud users about these topics so that their effectiveness is minimized. It is recommended that users be educated to recognize and handle social engineering techniques such as spear phishing that are commonly used to introduce APTs. Awareness programs that are regularly reinforced are one of the best defenses against these types of attacks, because some vulnerability requires user intervention or action. Staff should be ingrained with	

Area	Analysis
	thinking twice before opening an attachment or clicking a link. **Testing**: Please see testing technical recommendations for the Web-Based Attack consideration. In addition, configuration management is critical for the protection against APTs. **Monitoring and Detection**: It is recommended that, similarly to on premise networks, an Agency monitor for web-based attacks via any log, or other, monitoring data they gather from their cloud instances. **Notifications between Agency and CSP**: It is unknown how a given CSP will react to an APT in terms of notifying customers, possibly depending on the circumstances of the attack. During a previous test performed by DHS on an actual IaaS instance, one CSP detected intentional port scanning, shut down the cloud service, and notified the DHS customer that this was occurring. The same port scanning test was performed at a different CSP and the port scanning was not detected (i.e. the cloud service was not shut down and the customer was not notified). During another test of the 1st CSP (detected port scanning and notified customer), a sudden increase in traffic was detected by the CSP as a possible DOS attack and the cloud service was shut down but the customer was not notified. These data indicate that Agencies can expect a degree of variability in a CSPs ability to detect and to react to potential malicious attacks. It is recommended that Agencies work with their CSPs to understand the roles and responsibilities for detection and notification of potential malicious activity. An agency will likely want to know all that they can from the CSP if an APT is detected. Similarly, communication lines should be clearly established for scenarios where the Agency detects potential malicious activity in their instances (particularly PaaS and IaaS) and their responsibilities for notifying the CSP that something malicious is potentially occurring. For additional mitigation strategies, please see the following publication: Classification of APT's and Methodological Approach to Secure Cloud Services.[218]
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the implementation and assessment of the controls listed below— implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). NIST 800-53 advises > To more fully address the advanced persistent threat, concepts such as insider threat protection (CM-5(4)), heterogeneity (SC-29), deception (SC-26 and SC-30), non-persistence (SC-25 and SC-34), and segmentation (SC-7(13)) can be considered. (NIST 800-53, pages 37-8)

[218] https://www.ripublication.com/ijaer16/ijaerv11n2_41.pdf

Area	Analysis
	Particular attention should be given to • AC-6(9) Least Privilege | Auditing Use of Privileged Functions, • SC-30(3) Concealment and Misdirection | Change Processing / Storage Locations • SI-14 Non-Persistence • PM-16 Threat Awareness Program The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	Carbanak APT attack against financial institutions.[219] Additional articles that provide further discussion of APT threats, impacts and mitigations.[220,221]

Denial of Service

Overview

Similar to a traditional on-premise network attack, a denial of service attack (DoS) can execute in a variety of ways, such as sending an enormous volume of traffic to a server thereby overwhelming it and causing it to become incapable of responding to requests.

In 2016, the CSA considered the DDoS attacks in the cloud[222]:

> *Denial-of-service (DoS) attacks are attacks meant to prevent users of a service from being able to access their data or their applications. By forcing the targeted cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker—or attackers, as is the case in distributed denial-of-service (DDoS) attacks—causes an intolerable system slowdown and leaves all legitimate service users confused and angry as to why the service is not responding.*

Although a DOS attack in the commercial cloud is fundamentally similar to a DOS attack in an on-premise network, the cloud-specific multitenancy characteristics of cloud environments represent unique attack effects from this attack. For on premise networks, separate individual DOS attacks would be required to affect multiple organizations. In contrast, in a multitenant cloud environment, one DOS attack has the potential to affect multiple tenants. If an Agency is using a SaaS service in a multitenant environment, it may not even need to be the target of the attack to have its data and service affected, and is simply collateral damage from an attacker targeting a co-tenant.

This cloud consideration is impacted by the cloud characteristics: CSP Interdependency, Distribution of Data, One-to-Many, and Many-to-One.

---

[219] https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/
[220] https://www.scmagazine.com/report-exposes-apt-10s-cloud-hopper-campaign/article/648775/
[221] https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf
[222] https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

Analysis

Area	Analysis	
Cloud Service Model Considerations	*SaaS* *PaaS* *IaaS*	DOS attacks are applicable in SaaS, PaaS, and IaaS environments. Please see APT and Web-Based Attacks considerations for more information.
Risk Analysis	*Loss of Confidentiality, Integrity, and Availability*	A DOS attack in the cloud can lead to a loss of availability of Agency data.
	Risk to NIST Framework Implementation	The Denial of Service consideration can impact Risk Assessment ID.RA, Risk Management Strategy ID.RM, Identity Management, Authentication and Access Control PR.AC, Data Security PR.DS, Information Protection, Processes and Procedures PR.IP, Protective Technology PR.PT, Anomalies and Events DE.AE, Security Continuous Monitoring DE.CM, Detection Processes DE.DP, Communications RS.CO, and Analysis RS.AN.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to address the challenge of a Denial of Service Attack. • How do the service providers and consumers define a DOS attack in the cloud? • What are the roles and responsibilities of stakeholders regarding the disclosure of information pertaining to DOS attack in the cloud? • Through what channels will an Agency be notified that a DOS attack has taken place against the CSP? Will they only be notified if Agency data/services are impacted? • How can Agencies assess the ability of the CSP to detect, respond to, and recover from a DOS attack? • What security measures are employed by the CSP regarding data loss prevention and data security to limit the long-term impacts of a DOS attack? • What are the expectations regarding the speed with which the CSP can restore partial or full service following a DOS attack?	
Cloud Guidance	Please see the Advanced Persistent Threat and Web-Based Attacks considerations for more guidance.	
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the implementation and assessment of the controls in the System and Communications Protection (SC) control family (especially control SC-5 Denial of Service Protection)—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.	
Supporting Data	CSA The Treacherous 12 (2016): "[CSP] was suffering from a highly sophisticated attack by a group of unknown hackers, who had found a way to reverse engineer proof-of-concept code and create an easily-accessible backdoor for themselves into [CSP's]	

Area	Analysis
	massive bank of available processing power." Original source.[223] CSA The Treacherous 12: "In what looks like a series of co-ordinated cyber-attacks by a criminal gang, three major cloud-based services have all been knocked offline in recent days."Original Source.[224] "A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing."[225]

Incomplete Attack Information

Overview

Agencies in an on-premise environment have access to all the information associated with an attack on their network, services or applications. However, in a cloud environment, the CSP may circumvent an attack on an Agency after the attack has started. Because of the intervention of the CSP, the Agency is less likely to have a complete understanding or scope of such an incident. Therefore, it will have incomplete information regarding the attack.

The detection, response, and recovery actions taken when faced with an attack require the gathering of a great deal of information, some of which a CSP may be disinclined to share with an Agency. CSPs may block only part of an attack which diminishes an Agency's ability to fully characterize the incident and detect similar attacks in the future. Even if a CSP is aware of the complete attack and blocks all of it, they may not be willing to share all of the attack details with all customers. Some SLAs specify that a CSP is required to report on what has affected a customer's data only, which may only be a part of the attack. If an enterprise is compiling indicators and strategies based on known threats, but the enterprise does not know of all aspects of an attack, crafting a complete mitigation strategy is then challenging to create and to implement.

Agencies are likely to seek out all of the information available concerning a known attack; thus, they should work with their CSPs to determine what level of attack reporting is needed. For example, an Agency might want all information possible on a potential APT, but may not want to know about each and every event that the CSP logs.

This cloud consideration is impacted by the cloud characteristics: CSP Interdependency, Distribution of Data, One-to-Many and Adaptable to Multiple CSPs.

Please also see the cloud consideration "Reduced Capability to Perform Post-Event Forensics" for additional information.

Analysis

Area		Analysis
Cloud Service Model Considerations	*SaaS*	Incomplete Attack Information can affect SaaS, PaaS, and IaaS service models.
	PaaS	
	IaaS	
Risk Analysis	*Loss of*	This cloud consideration can lead to loss of the availability,

[223] https://vpncreative.net/2014/07/29/hackers-sneak-back-aws-ddos-launch-hub/
[224] http://www.ibtimes.co.uk/feedly-knocked-offline-by-ddos-attack-following-evernote-deezer-attacks-1452237
[225] www.mdpi.com/1999-5903/9/3/43/pdf

Area	Analysis	
	Confidentiality, Integrity, and Availability	confidentiality, and integrity of Agency data.
	Risk to NIST Framework Implementation	This cloud consideration may impact Governance ID.GV, Protective Technology PR.PT, Communication RS.CO, Analysis RS.AN, Mitigation RS.MI, and Improvements RS.IM.
Considerations to Guide Recommendations	The following questions can guide an Agency's ability to address the challenge of Incomplete Attack Information. • How do the service providers and consumers define an "incident" or "attack" in the cloud? • What are the roles and responsibilities of stakeholders regarding the disclosure of information pertaining to malicious attacks in the cloud? • What are essential pieces of information Agencies should request following notification that an attack took place? • How can Agencies assess the cybersecurity capabilities of a CSP if the CSP does not have to disclose information concerning attacks that do not target Agency data? • What security measures are employed by the CSP regarding data encryption, authentication, account management, etc.? • What is the responsibility of a consumer to report an incident? • What criteria must be met for a CSP to report an attack that it prevented or attempted to prevent to a customer?	
Cloud Guidance	In addition to relevant guidance already mentioned in the APT, DOS, and Web-Based Attack consideration guidance sections, it is recommended that Agencies work with their CSPs to determine what level of attack reporting is needed based on the magnitude of the detected attack. Taken from APT consideration analysis: **Notifications between Agency and CSP**: It is unknown how a given CSP will react to an APT in terms of notifying customers, possibly depending on the circumstances of the attack. During a previous test performed by DHS on an actual IaaS instance, one CSP detected intentional port scanning, shut down the cloud service, and notified the DHS customer that this was occurring. The same port scanning test was performed at a different CSP and the port scanning was not detected (i.e. the cloud service was not shut down and the customer was not notified). During another test of the 1st CSP (detected port scanning and notified customer), a sudden increase in traffic was detected by the CSP as a possible DOS attack and the cloud service was shut down but the customer was not notified. These data indicate that Agencies can expect a degree of variability in a CSPs ability to detect and to react to potential malicious attacks. These data indicate that in some cases, a CSP will not report attack details or even suspected DOS activity to a customer, creating incomplete attack information. It is recommended that Agencies work with their CSPs to understand the roles and responsibilities for detection and notification of potential malicious activity. An agency will likely want to know all that they can from the CSP if an APT is detected. Similarly, communication lines should be clearly established for scenarios where the Agency detects potential malicious activity in their instances (particularly PaaS and IaaS) and their responsibilities for notifying the CSP that something malicious is potentially occurring.	

Area	Analysis
Applicable FedRAMP Controls	The System Security Plan (SSP) for a CSO describes the CSP's implementation of the relevant FedRAMP baseline, which is based on the controls in NIST 800-53. A Security Assessment Report (SAR) provides an assessment by a Third-Party Assessment Organization (3PAO) of that implementation of that SSP. If an agency finds that the results of the assessment—particularly, for this consideration, the implementation and assessment of the controls in the Audit and Accountability (AU) and the Incident Response (IR) control families—implies that using the CSO represents an acceptable risk, then the agency should be in a position to grant Authority To Operate (ATO). This consideration may require modifying the SLA with the CSP to ensure that the CSP provides the needed level of detail. The agency should be attentive to the continuous and monitoring required for all CSOs. See the "Continuous Monitoring Strategy Guide," available at fedramp.gov.
Supporting Data	Internal testing of CSP services highlighted this cloud security consideration, external supporting data is not provided.