

---

Cloud Center  
of Excellence

# Common Federal Contracting Issues and Guidance for Procuring Cloud



---

DRAFT  
9.5.2017

---

# Common Federal Contracting Issues and Guidance for Procuring Cloud

## CLOUD CONTRACTING

### Introduction

**Note: the intent of this document is to provide information on issues encountered when contracting for cloud services from the commercial marketplace. The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses. This document should not be used as a “copy/paste document” or a contract solution.**

This document provides recommendations that can be considered for cloud implementations. Each issue should be addressed depending on the service model (IaaS, PaaS, SaaS) and the deployment model. Public cloud with services provided for general public use and accessed by any entity or organization willing to contract for it will require minimal guidance and requirements while community, hybrid, and private cloud models will require more studied and customized consideration.

The adoption of cloud within the federal government represents a dramatic shift in the way the federal government buys IT – a shift from periodic capital expenditures to lower cost and predictable operating expenditures. Civilian agencies must respond to this shift in the way they procure IT by adjusting the methodology by which we acquire IT from commercial providers.

The issues and recommendations contained in this document are intended to provide agencies with guidance to effectively acquire cloud computing and to focus on ways to procure cloud services within existing guidance, regulations and laws.

By highlighting the areas in which cloud computing presents unique requirements compared to the traditional IT contracts, this guidance will help to improve agency adoption of commercial cloud computing. By understanding these unique requirements and considering this guidance, agencies can implement dependable cloud computing contracts that deliver better outcomes for the federal government at a lower cost.

**The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.**

## ISSUES TO ADDRESS IN CIVILIAN CLOUD CONTRACTS

- PHYSICAL ACCESS
- PERSONNEL ACCESS
- NON-DISCLOSURE AGREEMENTS
- ASSET AVAILABILITY
- BANNER
- MISUSE OF GOVERNMENT DATA AND METADATA
- CONTINUOUS MONITORING
- DATA BREACH AND INCIDENT REPORTING
- FACILITY INSPECTIONS
- CYBERSECURITY COMPLIANCE
- USE OF SUBCONTRACTORS
- INDEMNIFICATION
- INSURANCE
- LOCATION OF DATA
- LAW ENFORCEMENT
- MAINTENANCE
- NOTIFICATION
- RECORDS
- SPILLAGE
- SUPPLY CHAIN
- TERMS OF SERVICE
- SERVICE LEVEL AGREEMENTS

## DEFINITIONS

access [CNSSI 4009]	Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.
configuration control	Having the authority to approve or disapprove any and all changes to the hardware and software used in the data repository systems.
compromise [CNSSI 4009]	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
data breach	The loss of control, compromise, unauthorized acquisition, unauthorized access, or any similar term referring to situations where any person has access or potential access to Government data under this contract, whether in electronic or non-electronic form, for any unauthorized purpose.

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

government data	Any document, media, or machine readable material regardless of physical form or characteristics that is created or obtained in the course of official government business.
government-related data	Any document, media, or machine readable material regardless of physical form or characteristics that is created or obtained by the contractor about or impacting the government data. This does not include contractor's business records e.g. financial records, legal records etc. or data such as software coding or algorithms that are not uniquely applied to the Government data.
isolate	To forensically segregate, store, manage, and maintain data separate and apart from any other data to preserve information integrity and prevent interaction.
National Agency Check with Inquiries (NACI)	The basic and minimum investigation required by the Federal government for employees and contractor under HSPD -12.
operational control	Having the authority over the components of the data repository systems to include the hardware, software, processes and personnel used to process or store government data.
Personally Identifiable Information (PII)	Data that can be used to distinguish or trace an individual's identity: such as name, social security number, date and place of birth, mother's maiden name, and bio-metric records, which are collected and maintained by an agency, including, but not limited to, education; financial transactions; and medical, criminal, or employment history.
spillage [CNSSI 4009]	Security incident that results in the transfer of classified or CUI information onto an information system not accredited (i.e., authorized) for the appropriate security level.

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

## Cloud Contract Guidance

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

### 1. PHYSICAL ACCESS

---

Issue:	Physical Access
Description:	The Agency needs to have physical access to a CSP data center to conduct inspections for FISMA, other audit purposes, or Inspector General investigations. These audits may be unannounced, so the Agency should ensure that its auditors have the access they need to complete their audits and investigations.
Applicability:	All cloud contracts
Rationale:	Inspector General Act of 1978 Federal Information Security Management Act of 2002 (FISMA) NIST 800-53
Proposed Contract Language:	<p>(1) The Contractor shall record all physical access to the cloud storage facilities and all logical access to the government data as specified in the contract. This may include the entrant's name, role, purpose, account identification, entry and exit time. Such records shall be provided to the Contracting Officer or designee in accordance with the contract or upon request to comply with federal authorities.</p> <p>(2) As specified by the Contracting Officer, the Contractor shall provide immediate access to all Government data and Government-related data impacting Government data for review, scan, or conduct of a forensic evaluation and physical access to any contractor facility with Government data. If the Government data is co-located with the non-Government data, the Contractor shall isolate the Government data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Government personnel identified by the Contracting Officer, and without the Contractor's involvement.</p>

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

## 2. PERSONNEL ACCESS

---

Issue:	Personnel Access
Description:	To further protect government data, the Agency should require all CSP employees who have access to government data, architecture that supports government data, or any physical or logical devices/code be U.S. person per Executive Order 12333 and pass an appropriate background check as required by Homeland Security Presidential Directive -12.
Applicability:	All cloud contracts
Rationale:	NIST 800-52 Rev4- Control PS-3: Personnel Screening HSPD-12
Proposed Contract Language:	The Contactor will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Government in compliance with HSPD -12. At a minimum, all Contractor employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.

## 3. NON-DISCLOSURE AGREEMENTS

---

Issue:	Non-Disclosure Agreements
Description:	The Agency should require CSP employees with access to government data and other government confidential information to sign a non-disclosure agreement that would legally prevent a CSP employee from disclosing non-public government information.
Applicability:	All cloud contracts
Rationale:	Maintaining confidentiality of government data and information. 5 CFR 2635.703 prohibits Federal employees from releasing non-public information; a NDA is the equivalent for contractor personal.

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

Contract Language: See number 6, *Organizational Conflict of Interest*. Ensure that all contractors sign an NDA.

#### 4. ASSET AVAILABILITY

---

Issue:	Asset availability
Description:	The Agency should ensure that the service level agreement with the CSP contains provisions for asset availability. The level of asset availability will be determined by the Agency's requirements.
Applicability:	All cloud contracts
Rationale:	Maintaining availability of government information and continuity of operations
Proposed Contract Language:	<p>The Contractor must inform the Government of any interruption in the availability of the cloud service as required by the service level agreement.</p> <p>Whenever there is an interruption in service, the Contractor must inform the Government of the estimated time that the system or data will be unavailable. The estimated timeframe for recovery of the service must be related to the FIPS 199 system categorization for the availability of the system and if specified, agreed upon service level agreements (SLA) [see number 22, <i>Service Level Agreements</i>] and system availability requirements. The Contractor must provide regular updates to the Government on the status of returning the service to an operating state according to the agreed upon SLAs and system availability requirements.</p> <p>The Contractor shall be responsible for maintaining and ensuring continued compatibility and interoperability with the Government's systems, infrastructure, and processes for the term of the contract. In the event of an unavoidable compatibility and interoperability issue, the Contractor shall be responsible for providing timely notification to the Government and shall be responsible for working with the Government to identify appropriate remedies and if applicable, work with the Government to facilitate a smooth and seamless transition to an alternative solution and/or provider.</p>

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

## 5. BANNER

---

Issue:	Banner
Description:	Banners or consent to monitor language allows Federal law enforcement the right to access and review government data including email created on a government system without a warrant or a subpoena. When a Government is only procuring hosting, the banner will be a requirement of the government or contractor who developed the system. However, when the government procures software as a service, the Agency should require the CSP to display the Agency's approved banner language prior to allowing a user access to the system.
Applicability:	Software as a Service (SaaS) contracts
Rationale:	Standard mandatory notice and consent banners should be displayed at logon to all ISs and standard mandatory notice and consent provisions should be included in all information system user agreements. The banner language provides consent for government to view any content on the system without a warrant.
Proposed Contract Language:	<p>The Standard Mandatory Notice and Consent Banner will be displayed at log on to all information systems. Choose either banner "a" or "b" based on the character limitations imposed by the system. The formatting of these documents, to include the exact spacing between paragraphs, must be maintained. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."</p> <p>[Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters.]</p> <p>You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.</p> <p>By using this IS (which includes any device attached to this IS), you consent to the following conditions:</p> <ul style="list-style-type: none"><li>-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.</li></ul>

**The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.**

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

OK

[For Blackberries and other PDAs/PEDs with severe character limitations:]

I've read & consent to terms in IS user agreem't.

## 6. MISUSE OF GOVERNMENT DATA AND METADATA

---

Issue:	Misuse of Government Data and Metadata
Description:	When the government places non-public information on a commercial cloud, the Agency should ensure the CSP refrains from using government data and any government specific metadata derived from the government's use of their service for any purpose other than expressly stated in the requirements
Applicability:	All cloud contracts
Rationale:	FAR 9.5 on Organizational Conflict of Interest prohibits a contractor from using information from its government work for other commercial needs.

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

Proposed Contract Language:

- (1) The Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract or a task order issued hereunder. If authorized by the terms of this contract or a task order issued hereunder, any access to, or use or disclosure of, Government data shall only be for purposes specified in this contract or task order. Contractor shall ensure that each of its employees and representatives, and any others (e.g., subcontractor employees) performing duties hereunder, shall, prior to obtaining access to any Government data, sign a contract or task order specific nondisclosure agreement.
- (2) The Contractor shall use Government-related data only to manage the operational environment that supports the government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

A breach of the obligations or restrictions set forth in (1) and (2) may subject the Contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and any other appropriate remedies by any party adversely affected by the breach.

## 7. CONTINUOUS MONITORING

---

Issue:	Continuous Monitoring
Description:	FedRAMP has mandated certain requirements for continuous monitoring in the "Continuous Mentoring Strategy Guide". These requirements require the CSP to produce certain reports and provide them to FedRAMP PMO and/or the FedRAMP 3PAO. The government client needs to request copies of these reports in its requirements (PWS/SOW), as the Agency's designated security point of contact is ultimately responsible for the protection of the data.
Applicability:	All cloud contracts
Rationale:	FISMA states that the Agency is responsible for accepting the risk for an IT system.
Proposed Contract Language:	The Contractor will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Government may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements. If requested, the Contractor will provide the report to the Government within 10 business days.

## 8. DATA BREACH AND INCIDENT REPORTING

---

Issue:	Data Breach/PIA
Description:	As with any IT system there is always a risk of a data breach. As such, the Agency should require the CSP to provide a plan for handling such a breach. If the breach includes PII, the contractor is required to notify the Agency of a breach within 60 minutes if the breach include PII (US Cert Requirement). In addition, the Agency is required to conduct a Privacy Impact Assessment (PIA) on all its IT systems. The purpose of the PIA is to analyze how information in identifiable form is handled: to ensure that its handling conforms to applicable legal, regulatory, and policy requirements for privacy; to determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system; and to examine and evaluate protections and alternative processes for handling such information to mitigate potential privacy risks. To assist the Agency in developing the PIA, the CSP should be required to provide the Agency with any required data about the CSP environment.
Applicability:	All cloud contracts
Rationale:	60, Cyber Incident Handling Program, Memorandum M-07-16, May 22, 2007, for safeguarding against and responding to breaches of PII; FISMA; requirements for agency incident response plans and reporting to the Federal information security incident center established by the Act, i.e., United States-Computer Emergency Readiness Team (US-CERT), within the Department of Homeland Security. See 44 U.S.C. 3544(b)(7), 3546.
Proposed Contract Language:	The Contractor will submit reports of cyber incidents through approved reporting mechanisms. The Contractor's existing

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

notification mechanisms that are already in place to communicate between the Contractor and its customers for some or all classes of CND information may be used, as long as those mechanisms demonstrate a level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

The Contractor will a template format when reporting initial incidents by secure fax, telephonically, or by other electronic means. Initial reports may be incomplete. Reporting should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.

In addition to the above, if the incident concerns a breach of PII or a potential breach of PII, the Contractor will report to the contracting officer's designee within 60 minutes of the discovery of any data breach. The Contractor shall provide the Government with all information and cooperation necessary to enable compliance by the Contractor and/or the Government with data breach reporting and mitigation actions required by applicable law, regulation, policy, and this contract.

## 9. FACILITY INSPECTIONS

---

Issue:	Facility Inspections
Description:	FISMA policy requires that facilities hosting Government data meet certain security standards. Routine inspections ensure that facilities are in compliance with these standards. Usually these inspections are conducted by the government; however, in the case of a CSP the government may agree to allow a third party to conduct an inspection based on the government's criteria.
Applicability:	All cloud contracts
Rationale:	Inspector General Act of 1978  FISMA
Proposed Contract Language:	The Contractor agrees to have an independent third party or other industry recognized firm, which has been approved by the Government conduct a security audit based on the Government's

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

criteria at least once a year. The audit results and Contractor's plan for addressing or resolving of the audit results shall be shared with the Government within 20 days of the Contractor's receipt of the audit results. In addition, the Government reserves the right to inspect the facility to conduct its own audit or investigation.

## 10. CYBERSECURITY COMPLIANCE

---

Issue:	Cybersecurity Compliance
Description:	It is important to inform CSP's that when hosting government data, they must comply with the FISMA and subsequent Agency policies
Applicability:	All cloud contracts
Rationale:	Maintaining the confidentiality, integrity and availability of Government information through FISMA Cybersecurity Policies
Proposed Contract Language:	<p>The Contractor will ensure that its environment is compliant with the control standards of FISMA (Federal Information Security Management Act) 44 U.S.C. § 3541, et seq.), NIST standards in FIPS 140-2, FIPS 180, FIPS 198-1, FIPS 199, FIPS 200, FIPS 201 and NIST Special Publications 800-53, 800-59, and 800-60. In addition, the Contractor must provide the Government with any documentation it requires for its reporting requirements within 10 days of a request.</p> <p>The Contractor will make the environment accessible for an Agency security team to evaluate the environment prior to the placement of any Government data in the environment and allow for periodical security reviews of the environment during the performance of this contract.</p>

## 11. USE OF SUBCONTRACTORS

---

Issue:	Use of Subcontractors
Description:	When subcontracting, the Agency should ensure the prime retains operational configuration and control of Government data.

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

Contractual liability to the government only exists with the prime contractor. When the government acquires a commercial service through an intermediary (e.g., system integrator, value added reseller), only the intermediary is accountable to the government. This reduces the contractual liability to the commercial service provider acting as the subcontractor, but increases the risks to the government.

Applicability:	All cloud contracts
Rationale:	Common law theory of privity of contract. The government needs to be in a contract with the host of the data.
Proposed Contract Language:	The Contractor shall retain operational configuration and control of data repository systems used to process and store government data to include any or remote work. The Contractor shall not subcontract the operational configuration and control of any government data.

## 12. INDEMNIFICATION

---

Issue:	Indemnification
Description:	Indemnification by the CSP protects the government when third parties sue the government for a tort when the CSP, not the government was liable. Indemnification also allows the government to recoup any costs related to a third party law suit.
Applicability:	All cloud contracts
Rationale:	Sovereign Immunity clause of the Constitution Article III Section II. The government has not granted immunity to be sued for actions by third parties. See also the Federal Torts Claim Act.
Proposed Contract Language:	The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of the Contractor's unauthorized introduction of copyrighted material, information subject to a right of privacy, and any libelous or other unlawful matter into Government data. The Contractor agrees to waive any and all defenses that may be asserted for its benefit, including (without limitation) the Government Contractors Defense.

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of (i) the Contractor's unauthorized disclosure of trade secrets, copyrights, contractor bid or proposal information, source selection information, classified information, material marked "For Official Use Only", information subject to a right of privacy or publicity, personally identifiable information as defined in OMB Memorandum M-07-19 (July 12, 2006), or any record as defined in 5 U.S.C. § 552a; or (ii) the Contractor's unauthorized introduction of any libelous or other unlawful matter into Government data. The contractor agrees to waive any and all defenses that may be asserted for its benefit, including without limitation the Government Contractors Defense.

In the event of any claim or suit against the Government on account of any alleged unauthorized disclosure or introduction of data or information arising out of the performance of this contract or services performed under this contract, the Contractor shall furnish to the Government, when requested by the Contracting Officer, all evidence and information in the Contractor's possession pertaining to such claim or suit. Such evidence and information shall be furnished at the expense of the Contractor; provided, however, that an equitable adjustment shall be made under this clause, and the contract modified in writing accordingly, if the claim or suit is withdrawn, settled, or adjudicated in favor of the Government, and the basis for the claim or suit, regardless of outcome, was not due to any act or omission of the Contractor.

The provisions of this paragraph do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Contractor's consent to the settlement of any claim or suit other than as required by final decree of a court of competent jurisdiction; and these provisions do not apply to any libelous or other unlawful matter contained in such data furnished to the Contractor by the Government and incorporated in data to which this clause applies. Further, this indemnity shall not apply to—

- A disclosure or inclusion of data or information upon specific written instructions of the Contracting Officer directing the disclosure or inclusion of such information or data;

- A third-party claim that is unreasonably settled without the

consent of the Contractor, unless required by final decree of a court of competent jurisdiction.

### 13. INSURANCE

---

Issue:	Insurance
Description:	The Agency may require a CSP to have the necessary insurance to pay for any costs stemming from a breach of Government data or to replace any damages to the Government system
Applicability:	All cloud contracts
Rationale:	Liability insurance requirement.
Proposed Contract Language:	<p>The Contractor shall provide and maintain insurance, to include cybersecurity insurance, throughout the performance of this contract, as specified in the Schedule or elsewhere in the contract.</p> <p>Before commencing performance under this contract, the Contractor shall provide proof of insurance to the Contracting Officer. The Contractor shall resubmit the proof of insurance within 30 days of notification of any material change that occurs during the performance of the contract.</p> <p>The Agency can require the Contractor to insert the substance of this language into subcontracts under this contract, and any subsequent subcontracts under those, that require work with or in support of storage and retrieval of electronic/digital government data and may require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. In the event of this requirement, the Contractor shall maintain a copy of all subcontractors' proofs of required insurance and shall make copies available to the Contracting Officer, or his/her designee, upon request.</p>

### 14. LOCATION OF DATA

---

Issue:	Location of Data
Description:	Government data can only be released by an authorized official or

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

by a court order from a US Federal Court. If a CSP places Government data in a foreign jurisdiction its servers would be subject to the laws of that jurisdiction and risks Government data being seized by a foreign government.

Applicability:	All cloud contracts
Rationale:	Sovereign Immunity under the Article III Section II of the Constitution. US Government data is sovereign and is not subject to other jurisdictions.
Proposed Contract Language:	<p>The Contractor shall maintain all data within the United States, which means the 50 States, the District of Columbia, and outlying areas.</p> <p>The Contractor shall provide the Government with a list of the physical locations which may contain government data within 20 days with updates on a quarterly basis.</p>

## 15. LAW ENFORCEMENT

---

Issue:	Law Enforcement
Description:	As mentioned in the Banner Issue above, all users to Government systems have consented through the banner language to monitoring of their use of a Government system and use of that data for law enforcement purposes. As such, Federal law enforcement officials do not need a warrant or a subpoena to access government data on a government system.
Applicability:	All cloud contracts
Rationale:	Inspector General Act of 1978 FISMA Law Enforcement Authorities
Proposed Contract Language:	The Contractor shall record all physical access to the cloud storage facilities and all logical access to the government data as specified in the Schedule. This may include the entrant's name, role, purpose, account identification, entry and exit time. Such records shall be provided to the Contracting Officer or designee in accordance with the Schedule or upon request to comply with

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

federal authorities.

As specified by the Contracting Officer, the Contractor shall provide immediate access to all Government data and Government-related data impacting Government data for review, scan, or conduct of a forensic evaluation and physical access to any contractor facility with Government data. If the Government data is co-located with the non-Government data, the Contractor shall isolate the Government data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Government personnel identified by the Contracting Officer, and without the Contractor's involvement.

## 16. MAINTENANCE

---

Issue:	Maintenance
Description:	Agencies should require CSPs to conduct regular maintenance including patches on its environment to prevent intrusions.
Applicability:	All cloud contracts
Rationale:	Best practice and a cybersecurity requirement
Proposed Contract Language:	The Contractor shall be responsible for all patching and vulnerability management (PVM) of software and other systems' components supporting services provided under this agreement so as to prevent proactively the exploitation of IT vulnerabilities that may exist within the Contractor's operating environment. Such patching and vulnerability management shall meet the requirements and recommendations of NIST SP 800-40, as amended, with special emphasis on assuring that the vendor's PVM systems and programs apply standardized configurations with automated continuous monitoring of the same to assess and mitigate risks associated with known and unknown IT vulnerabilities in the Contractor's operating environment. Furthermore, the Contractor shall apply standardized and automated acceptable versioning control systems that use a centralized model to capture, store, and authorize all software development control functions on a shared device that is accessible to all developers authorized to revise software supporting the services provided under this agreement. Such

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

versioning control systems shall be configured and maintained so as to assure all software products deployed in the Contractor's operating environment and serving the Government are compatible with existing systems and architecture of the Government.

## 17. NOTIFICATION

---

Issue:	Notification
Description:	Similar to jurisdiction, CSP data centers are subject to state and local law enforcement officials, and state and local subpoenas. The Agency should ensure the CSP notifies the Agency of a warrant or a subpoena so that the Department of Justice can protect Agency data from release.
Applicability:	All cloud contracts
Rationale:	Sovereign Immunity under the Article III Section II of the Constitution. US Government data is sovereign and is not subject to other jurisdictions.
Proposed Contract Language:	The Contractor shall notify the Government within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any Government data. The Contractor shall cooperate with the Government to take all measures to protect Government data from any loss or unauthorized disclosure that might reasonably result from the execution of any such warrant, seizure, subpoena, or similar legal process.

## 18. RECORDS

---

Issue:	Records
Description:	The Agency is required to maintain and produce records per the Federal Records Act, the Freedom of Information Act, and the Federal Rules of Civil Procedure. Records are kept based on the Agency's disposition schedule. The government should work with the CSP to ensure that all government records and CSP records

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

about government data are kept in accordance with Agency record's schedules.

Applicability: All cloud contracts

Rationale: Federal Records Act  
Freedom of Information Act  
Federal Rules of Civil Procedure

Proposed Contract Language: The Contractor shall provide the Contracting Officer all Government data and Government-related data in the format specified in the Schedule or as directed by the Contracting Officer.

The Contractor shall dispose of Government data and Government-related data in accordance with the Schedule and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

The Contracting Officer may at any time issue a hold notification in writing to the Contractor. At such time, the Contractor may not dispose of any Government data or Government-related data described in the hold notification until such time as the Contractor is notified in writing by the Contracting Officer, and shall preserve all such data in accordance with agency instructions.

The Contractor shall provide the Contracting Officer within 10 business days of receipt of any requests from a third party for Government-related data.

When the Government is using a Contractor's software, the Contractor shall provide the agency with access and the ability to search, retrieve, and produce Government data in a standard commercial format.

## 19. SPILLAGE

---

Issue: Spillage

Description: Occasionally, classified information spills over to an unclassified system. When this happens, the agency should ensure the CSP follows the procedures in CNSS 1001.

Applicability: All cloud contracts

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

Rationale:	Committee on National Security Systems Instruction (CNSSI) No. 1001, <i>National Instruction on Classified Information Spillage</i>
Proposed Contract Language:	<p>Upon written notification by the Government of a spillage, the Contractor shall coordinate immediately with the responsible Government official to correct the spillage in compliance with agency-specific instructions.</p> <p>If the Contractor incurs additional cost to correct the spillage, or the effort to correct the spillage causes a delay in the performance of any part of the work under this contract, and such costs or delays were not caused by any act or omission of the Contractor, an equitable adjustment shall be made under this clause and the contract modified in writing accordingly.</p> <p>No request by the Contractor for an equitable adjustment to the contract under this clause shall be allowed, unless the Contractor has given a written notice thereof within 30 days after the notification prescribed in paragraph (a) of this clause.</p> <p>No request by the Contractor for an equitable adjustment to the contract due to a spillage shall be allowed if made after final payment under this contract.</p> <p>Any spill of data by the Contractor into the environment hosting Government Data, will be immediately reported to the Government POC (insert POC) and the Contractor will follow the Government's instructions to clean up the spill at the Contractor's expense.</p>

## 20. SUPPLY CHAIN

---

Issue:	Supply Chain
Description:	The Agency should ensure CSPs exercise due diligence to use genuine hardware and software products that are free of malware.
Applicability:	All cloud contracts
Rationale:	HSPD 23 and NSPD 54
Proposed Contract Language:	Supply Chain Risk Management (SCRM) Plan. The offeror shall submit a SCRM plan as part of its technical proposal. The SCRM plan shall describe the offeror's approach to SCRM and demonstrate how

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

the offeror's approach will reduce and mitigate supply chain risks. The SCRM plan shall address:

**System Security Engineering.** The SCRM plan shall describe the offeror's use of system security engineering processes in specifying and designing a system that is protected against external threats and against hardware and software vulnerabilities.

**Criticality Analysis.** The SCRM plan shall include the criticality analysis (CA) process used by the offeror to determine Mission Critical Functions and the protection techniques (countermeasures and sub-countermeasures) used to achieve system protection and mission effectiveness. The CA shall describe the offeror's supply chain for all critical hardware and software components (and material included in products), key suppliers, and include proof of company ownership and location (on-shore or off-shore) for key suppliers and component manufacturers. The CA shall identify critical functions and components (hardware, software, and firmware).

**SCRM Security Controls.** The SCRM plan shall describe the offeror's strategy for implementing of SCRM security requirements throughout the life of the contract. The SCRM plan shall address the security controls (at a minimum SA-12) described in National Institute of Standards & Technology (NIST) Special Publication 800-53 Revision 4 (current version), Recommended Security Controls for Federal Information Systems and Organizations (<http://csrc.nist.gov/publications/PubsSPs.html>), and should be tailored in scope to the effort and the specific unclassified Government information.

**Delivery Mechanisms.** The SCRM plan shall describe the offeror's physical and logical delivery mechanisms to protect against unauthorized access, exposure of system components, information misuse, unauthorized modification, or redirection;

**Operational and Disposal Processes.** The SCRM plan shall describe the offeror's operational processes (during maintenance, upgrade, patching, element replacement, or other sustainment activities) and disposal processes that limit opportunities to knowledge exposure, data release, or system compromise.

**SCRM Training/Awareness Program.**

**Contractor-Manufacturer Relationship.** The SCRM plan shall identify the relationship between the offeror and the manufacturer as one of the following: (1) OEM; (2) authorized reseller; (3) authorized

partner/distributor; or (4) unknown/unidentified source.

Malicious Code Warranty. The SCRM plan shall include the offeror's expressed warranty that the software shall be free from all computer viruses, worms, time-outs, time bombs, back doors, disabling devices and other harmful or malicious code intended to or which may damage, disrupt, inconvenience or permit access to the software user's or another's software, hardware, networks, data or information.

Subcontracts. The Offeror shall incorporate the substance of this requirement in subcontracts at all tiers where a subcontractor provides personnel, components or processes identified as either a critical component or its supporting infrastructure. All subcontractors providing critical components or services shall be identified and required to provide all necessary information to complete the SCRM Plan in association with the Offeror.

SCRM Plan Submission & Review. The SCRM plan and supporting documents shall be submitted to the contracting officer as part of the offeror's technical proposal. All SCRM plans and appropriately marked related information will be treated as proprietary information by the Government and handled as Controlled Unclassified Information pursuant to Executive Order 13556 and shall be used solely for the purposes of managing risk to Government Functions. The government shall review the offeror's SCRM plan to determine whether the SCRM plan demonstrates an acceptable methodology for managing supply chain threats/risks. The SCRM plan review shall consider the offeror's SCRM approach for: (1) System Security Engineering; (2) Criticality Analysis; (3) SCRM Security Controls; (4) Delivery Mechanisms; (5) Operational and Disposal Processes; and (5) SCRM Training/Program Awareness. The SCRM plan must be deemed acceptable by the contracting officer in order for the offeror to be eligible for award. The offeror's failure to submit an acceptable SCRM plan may result in the offeror being eliminated from further consideration for contract award.

Material Term of the Contract. Failure by the offeror to submit an acceptable SCRM Plan with its proposal may result in the offeror's exclusion from award. Failure by the Contractor to execute, maintain and distribute a current SCRM Plan for review by the Government in accordance with the terms of the contract shall constitute a material breach of the contract and may result in termination for default or cause.

## 21. TERMS OF SERVICE

---

Issue:	Terms of Service
Description:	<p>Many commercial services have Terms of Service Agreements that contain clauses that the government cannot accept. Below are some examples:</p> <p><b>CONFIDENTIALITY</b> This is a clause where the government agrees not to release confidential information. However, the government is subject to the Freedom of Information Act and must follow its procedures to release or protect commercial information.</p> <p><b>INDEMNIFICATION</b> Many terms of service agreement contain an open ended indemnification clause where the government will indemnify the CSP against third party claims. This type of clause violates the Anti-Deficiency Act because the government is committing to funds that have yet to be appropriated. This clause needs to be re-worked to reference other applicable laws.</p> <p><b>GOVERNING LAW</b> Many terms of service agreements have the governing law for the agreement to be a specific state and have a venue for any disputes to be in that state's courts. As the Federal government is not subject to state law, it can only be sued in Federal court.</p> <p><b>ENDORSEMENT</b> Many terms of service agreements also have a clause where the CSP may quote / cite the government's use of its product as an endorsement or testimonial. The government does not endorse commercial products or services.</p>
Applicability:	All cloud contracts -- These get changed based on the providers Terms of Service (TOS).
Rationale:	<p>Freedom of Information Act</p> <p>Article I Section 8 of the US Constitution. Congress has to appropriate money.</p> <p>New FAR 52.212-4(u). 78 FR 80382</p> <p>Unenforceable Indemnifications- The government cannot commit to funds that have yet to be appropriated</p> <p>Sovereign Immunity under the Article III Section II of the</p>

The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.

Constitution. US Government data is sovereign and is not subject to other jurisdictions.

5 C.F.R. 2635.702, the Federal Acquisition Regulation (FAR) (48 C.F.R. §3.101-1), Executive Order 12731

Proposed Contract Language:

Use FAR Clause: 52.212-4(u): The following shall supersede any language in the Contractor's commercial terms of service:

- (1) Confidentiality. The Government, to the extent permitted by law and regulation, will safeguard and treat information obtained pursuant to the Contractor's disclosure as confidential where the information has been marked "confidential" or "proprietary" by the company. To the extent permitted by law and regulation, such information will not be released by the Government to the public pursuant to a Freedom of Information Act request, 5 U.S.C. § 552, without prior notification to the Contractor. The Government may transfer documents and information provided by the Contractor to any department or agency within the Executive Branch if the information relates to matters within the organization's jurisdiction.
- (2) Disputes and governing law. Any and all other terms or conditions notwithstanding, disputes arising under or relating to this contract or agreement are subject exclusively to Federal law, particularly the Contract Disputes Act of 1978, as amended (41 U.S.C. §§ 7101-7109) (the Act) and the provisions of 48 CFR subpart 33.2. Except as provided in the Act, all disputes arising under or relating to this contract shall be resolved under the clause set forth at 48 CFR 52.233-1.
- (3) Other legal matters. Any and all other terms or conditions notwithstanding, legal actions in which the Government is a party that do not arise under or relate to this contract or agreement shall be prosecuted under applicable Federal law in the appropriate Federal venue.
- (4) Endorsement. The Contractor may not use the name, seal, logo or other readily identifiable indicia of any Government agency or organization in such a way that may be construed as advertising or endorsement by the Government of the Contractor. The Contractor may include within a list or display of the Contractor's customers for the purposes of advertising or publicity the names, seals, logos or other indicia of Government agencies and organizations that have entered into contracts with the Contractor. However, it must not be

**The information is for consideration and is not intended to be contract language or official direction. Consult with your contracting officer regarding official language and clauses.**

stated or implied that the Government in any way recommends or endorses the products or services of the Contractor

- (5) Indemnification and renewal. Any other terms or conditions notwithstanding, this contract or agreement shall not and does not require the Government to (i) indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability, which would violate the Anti-Deficiency Act (31 U.S.C. § 1341) (ADA), or (ii) automatically renew this contract or agreement at any time in the future, which would violate the ADA. Any such provisions set forth in this contract or agreement are unenforceable against the Government.

## 22. SERVICE LEVEL AGREEMENTS

---

Issue:	Service Level Agreements
Description:	Federal and private sector guidance highlights the importance of federal agencies using a service level agreement (SLA) in a contract when acquiring information technology (IT) services through a cloud computing services provider. An SLA defines the level of service and performance expected from a provider, how that performance will be measured, and what enforcement mechanisms will be used to ensure the specified performance levels are achieved.
Applicability:	All cloud contracts – The consequences change based on the providers Service Level Agreements (SLAs).
Rationale:	GAO 16-325 “Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance”

Proposed Contract Language: See SLA related issues covering: identifying the roles and responsibilities of major stakeholders, defining performance objectives, specifying security metrics, and providing consequences for non-compliance with the SLA performance measures.

(1) Roles and Responsibilities

Without clearly defined roles, responsibilities, and terms, the agency may not be able to appropriately measure the cloud provider's performance.

- A. Specify roles and responsibilities of all parties with respect to the SLA, and, at a minimum, include agency and cloud providers.

Define the roles and responsibilities of the major stakeholders involved in the performance of the SLA and cloud contract. These definitions would include, for example, the persons responsible for oversight of the contract, audit, performance management, maintenance, and security.

- B. Define key terms, including activation date, performance, and identify any ambiguities in the definitions of cloud computing terms to provide the agency with the level of service they can expect from their cloud provider.

(2) Performance measures

Without any type of performance measures in place, agencies would not be able to determine whether the cloud services under contract are meeting expectations. Providing performance parameters provides both the agency and service provider with a well-defined set of instructions to be followed.

- A. Define clear measures for performance by the contractor. Include which party is responsible for measuring performance. Examples of such measures would include:

- (i) Level of service (e.g., service availability—duration the service is to be available to the agency).
- (ii) Capacity and capability of cloud service (e.g., maximum number of users that can access the cloud at one time and ability of provider to expand services to more users).
- (iii) Response time (e.g., how quickly cloud service

provider systems process a transaction entered by the customer, response time for responding to service outages).

- B. Specify how and when the agency has access to its own data and networks.
  - (i) Include how data and networks are to be managed and maintained throughout the duration of the SLA and transitioned back to the agency in case of exit/termination of service.
  - (ii) Provide any data limitations, such as who may or may not have access to the data and if there are any geographic limitations.
- C. Specify the following service management requirements:
  - (i) How the cloud service provider will monitor performance, report incidents, and how and when they would plan to resolve them and report results to the agency.
  - (ii) Identify how and when the agency would conduct an audit to monitor the performance of the service provider, including access to the provider's performance logs and reports.
- D. Provide for disaster recovery and continuity of operations planning and testing, including
  - (i) Performing a risk management assessment
  - (ii) how the cloud service would be managed by the provider in the case of a disaster
  - (iii) how data would be recovered; and what remedies would apply during a service failure.
  - (iv) how and when the cloud service provider is to report such failures and outages to the agency.
  - (v) how the provider will remediate such situations and mitigate the risks of such problems from recurring.
- E. Describe any applicable exception criteria when the cloud provider's performance measures do not apply (e.g., during scheduled cloud maintenance or when updates occur).

### (3) Security

Without these safeguards, computer systems and networks as well as the critical operations and key infrastructures they

support may be lost, and information—including sensitive personal information—may be compromised, and the agency’s operations could be disrupted.

- A. Specify the security performance requirements that the service provider is to meet to show it is meeting the agency’s security performance requirements for protecting data (e.g., clearly define who has access to the data and the protections in place to protect the agency’s data).
  - (i) This would include describing security performance metrics for protecting data, such as data reliability, data preservation, and data privacy.
  - (ii) Clearly define the access rights of the cloud service provider and the agency as well as their respective responsibilities for securing the data, applications, and processes to meet all federal requirements.
- B. Describe what would constitute a breach of security and specify performance requirements and attributes defining how and when the cloud service provider is to notify the agency when security requirements are not being met (e.g., when there is a data breach).

(4) Consequences

Without penalties and remedies, the agency may lack leverage to enforce compliance with contract terms when situations arise.

- A. Specify a range of enforceable consequences, such as penalties, for non-compliance with SLA performance measures.
- B. Include the terms under which a range of penalties and remedies would apply for non-compliance with the SLA performance measures.
- C. Identify how such enforcement mechanisms would be imposed or exercised by the agency.