Attachment 1. DAF Clauses

1. **Ombudsman (DAF Part 1)– required on all contracts** 1
2. **Elimination Of Use of Class I Ozone Depleting Substances (ODS) (DAF Part 23)** 2
3. **Health and Safety on Government Installations (DAF Part 23)** 2
4. **Notification of Government Security Activities (DAF Part 40)** 3
5. **Security Incident Reporting and Procedures (DAF Part 40)** 3
6. **Contractor Access to Department of the Air Force Installations (DAF Part 42)** 6
7. **Common Access Cards (CAC) for Contractor Personnel (DAF Part 42)** 8

1. **Ombudsman (DAF Part 1)– required on all contracts**
    a. An ombudsman has been appointed to hear and facilitate the resolution of concerns from offerors, potential offerors, and others for this acquisition. When requested, the ombudsman will maintain strict confidentiality as to the source of the concern. The existence of the ombudsman does not affect the authority of the program manager, contracting officer, or source selection official. Further, the ombudsman does not participate in the evaluation of proposals, the source selection process, or the adjudication of protests or formal contract disputes. The ombudsman may refer the interested party to another official who can resolve the concern.
    b. Before consulting with an ombudsman, interested parties must first address their concerns, issues, disagreements, and/or recommendations to the contracting officer for resolution. Consulting an ombudsman does not alter or postpone the timelines for any other processes (e.g., agency level bid protests, GAO bid protests, requests for debriefings, employee-employer actions, contests of OMB Circular A-76 competition performance decisions).
    c. If resolution cannot be made by the contracting officer, the interested party may contact the ombudsman, Colonel James Simmons, AFICC/KG, 801 Kenney Ave, Suite 2221, Barksdale AFB, LA 71110, phone number (701) 781-6336, email address james.simmons.6@us.af.mil, alternate email address ig.afica.kg.workflow@us.af.mil. Concerns, issues, disagreements, and recommendations that cannot be resolved at the Center/MAJCOM/FLDCOM/DRU ombudsman level, may be brought by the interested party for further consideration to the Department of the Air Force ombudsman, Associate Deputy Assistant Secretary (ADAS) (Contracting),

SAF/AQC, 1060 Air Force Pentagon, Washington DC 20330-1060, phone number (571) 256-2395, facsimile number (571) 256-2431.

d. The ombudsman has no authority to render a decision that binds the agency.
e. Do not contact the ombudsman to request copies of the solicitation, verify offer due date, or clarify technical requirements. Such inquiries shall be directed to the contracting officer.

2. Elimination Of Use of Class I Ozone Depleting Substances (ODS) (DAF Part 23)

a. General Prohibitions
   i. In accordance with Department of the Air Force (DAF) environmental policies, the Contractor must strictly avoid the use of Class I Ozone Depleting Substances (ODS). Specifically, the Contractor must not:
      1. Provide any service or product with any specification, standard, drawing, or other document that requires the use of a Class I ODS in the test, operation, or maintenance of any system, subsystem, item, component, or process.
      2. Provide any specification, standard, drawing, or other document that establishes a test, operation, or maintenance requirement that can *only* be met by the use of a Class I ODS as part of this contract or order.

b. Defined Class I ODS Products
   i. For the purposes of DAF policy, the following products that are pure (i.e., they meet the relevant product specification identified in AFI 32-7086, *Hazardous Materials Management*) are classified as Class I ODSs:

Category	Prohibited Substances
Halons	1011, 1202, 1211, 1301, and 2402
Chlorofluorocarbons (CFCs)	CFC-11, CFC-12, CFC-13, CFC-111, CFC-112, CFC-113, CFC-114, CFC-115, CFC-211, CFC-212, CFC-213, CFC-214, CFC-215, CFC-216, and CFC-217
CFC Blends	R-500, R-501, R-502, and R-503
Other Solvents & Fumigants	Carbon Tetrachloride, Methyl Chloroform, and Methyl Bromide

3. Health and Safety on Government Installations (DAF Part 23)

When performing work under this contract on a Government installation, the Contractor must comply with the following requirements:

a. General Precautions
   i. The Contractor must take all reasonable steps and precautions to prevent accidents and protect the health and safety of Contractor and Government personnel involved in, or coming into contact with, the performance of this contract.

b. Additional Directed Precautions
   i. The Contractor must take any additional immediate precautions that the Contracting Officer (CO) reasonably requires for health and safety purposes.

c. Application of Safety Standards

i. The CO may issue a written order directing the Contractor to adhere to Department of the Air Force Occupational Safety and Health (AFOSH) standards or other specific health and safety standards. Any contract adjustments resulting from these directed standards will be processed in accordance with the Changes clause of this contract.

d. Correcting Violations

i. Any violation of these health and safety rules and requirements is grounds for termination under the Default clause of this contract, unless the Contractor promptly corrects the violation as directed by the CO.

4. Notification of Government Security Activities (DAF Part 40)

a. DD Form 254 Applicability

i. This contract includes a DD Form 254, Department of Defense (DoD) Contract Security Classification Specification, and requires performance at a Government location in the U.S. or overseas. Before beginning operations that involve classified information on an installation identified on the DD Form 254, the Contractor must fulfill the notification requirements specified below.

b. Notification Requirements

i. At least thirty (days before beginning operations, the Contractor must notify the Information Protection Office listed in the distribution block of the DD Form 254. The notification must include:

1. The name, address, and telephone number of the Contractor's representative and designated alternate in the U.S. or overseas area, as appropriate.
2. The contract number and the military contracting command.
3. The highest classification category of defense information that Contractor employees will access.
4. The Department of the Air Force (DAF) installations in the U.S. where the contract work will be performed. (For overseas areas, the Contractor must identify only the Army Post Office (APO) numbers).
5. The date Contractor operations will begin on the base in the U.S. or in the overseas area.
6. The estimated completion date of operations on the base in the U.S. or in the overseas area.
7. Any subsequent changes to the information previously provided.

5. Security Incident Reporting and Procedures (DAF Part 40)

a. General Requirements

i. When this contract includes a DD Form 254, Department of Defense (DoD) Contract Security Classification Specification, the Contractor must comply with the following requirements:

ii. The Contractor must notify the Government Contracting Activity (GCA) of any security incident involving the potential, actual, or suspected loss or

compromise of classified information (Top Secret, Secret, or Confidential) discovered at the Contractor's location.

iii. The Contractor must conduct required inquiries in accordance with 32 CFR Part 117 and guidance from its Cognizant Security Office (CSO) (e.g., Defense Counterintelligence and Security Agency (DCSA)).

iv. For security incidents occurring at Government locations where the Contractor is categorized as a visitor, the Contractor must process and report the incident using the Government host's security procedures.

v. The GCA holds jurisdiction over security incidents involving Special Access Programs (SAP) or Sensitive Compartmented Information (SCI). For these incidents, the Contractor must follow specific GCA guidance instead of these standard requirements.

vi. These requirements do not relieve the Contractor from reporting requirements or security guidance mandated by 32 CFR Part 117, DFARS 252.204-7012, the contract, or the CSO.

vii. The Contractor must ensure all applicable subcontracts include these security incident reporting requirements.

viii. If compromised information is unrecoverable and outside U.S. Government jurisdiction (e.g., media leaks, public website postings, or loss in a foreign country), the Contractor must classify the notification and the geographic location of the compromise at the same level as the compromised material, per DoDM 5200.01 Volume 3, Enclosure 6. In all such cases, the Contractor must contact the GCA for communication instructions before submitting the notification.

ix. The Contractor must ensure all notifications containing classified information are properly transmitted and marked according to derivative classification and overarching marking guidelines in 32 CFR Part 117.

b. Initial Notification of Security Incident

i. Unless the contract directs otherwise, the Contractor must provide an initial notification to the GCA within 72 hours of discovering any security incident at the Contractor's location where classified information may have been lost or compromised.

ii. The initial notification is Controlled Unclassified Information (CUI) [CUI category OPSEC, FEDCON Distribution/Dissemination Control] unless the GCA determines otherwise. The Contractor must mark it in accordance with DoDI 5200.48 and transmit it to the GCA through authorized means (e.g., encrypted email or DoD SAFE).

iii. If the initial notification contains classified information (either by content or compilation), the Contractor must contact the GCA for submission guidance and ensure proper marking per 32 CFR Part 117.

iv. The initial notification must contain the following information, as available:

1. Prime contract number associated with the incident.
2. Date the security incident occurred.

3. Date of discovery (if different from the date of occurrence).
4. Security Classification Guide (SCG) or guidance used to validate the classification level (unclassified title and date). Note: If the SCG title is classified, or if listing the information classifies the notification by compilation, the Contractor must omit the SCG title and explicitly state the reason for omission.
5. Classification level of the information involved (e.g., Top Secret, Secret, Confidential).
6. A brief description of the incident. If Government personnel were involved, include their names, email addresses, and office information.
7. A statement indicating whether the Contractor can retain or provide the suspected information for GCA classification review or damage assessment.

c. Final Notification of Security Incident
   i. The Contractor must provide a final notification to the GCA within ten (10) business days of the initial notification. If the Contractor cannot meet this deadline, it must request and receive written approval for an extension from the GCA.
   ii. The final notification does not relieve the Contractor from reporting requirements mandated by 32 CFR Part 117, DFARS 252.204-7012, the contract, or the CSO.
   iii. The final notification is CUI unless the GCA determines otherwise. The Contractor must mark it per DoDI 5200.48 and send it through authorized means.
   iv. If the final notification contains classified information, the Contractor must contact the GCA for submission guidance and mark it per 32 CFR Part 117.
   v. The final notification must contain the following information:
      1. Prime contract number.
      2. Date of occurrence and date of discovery.
      3. SCG or guidance used (subject to the same classification restrictions as 6.2.4.4).
      4. Classification level of the information involved.
      5. A detailed description of the incident, including: the sequence of events (when, where, and how); contributing persons, situations, or conditions; details of any involved Government personnel; steps taken to locate physically lost material; and measures taken to sanitize assets if a data spill occurred.
      6. Corrective actions taken to prevent future occurrences.
      7. Result of the inquiry (e.g., loss, compromise, suspected compromise, or no compromise).
      8. A copy of the supporting DD Form 254(s). If the Contractor cannot provide the form, it must state the reasons why in the report.

d. Definitions
    i. 32 CFR Part 117: National Industrial Security Program Operating Manual.
    ii. Business days: Days excluding Federal holidays and weekends.
    iii. Classified information: Information designated by the Government as requiring protection against unauthorized disclosure in the interest of national security. This includes national security information (NSI), restricted data (RD), and formerly restricted data (FRD), regardless of physical form.
e. Cognizant Security Agencies (CSAs): Agencies with National Industrial Security Program implementation responsibilities, including DoD, DOE, NRC, ODNI, and DHS.
f. Cognizant Security Office (CSO): An organizational unit delegated to administer industrial security services on behalf of a CSA.
g. Compromise: An unauthorized disclosure of classified information.
h. Data spill: The electronic transmission of classified information via unsecure means (e.g., over an unclassified network).
i. Derivative classification: Incorporating, paraphrasing, restating, or generating classified information in a new form and marking it consistently with the source information.
j. Government Contracting Activity (GCA): A designated component element with broad acquisition authority (including Contracting Officers, program managers, and security personnel).
k. Inquiry: The initial fact-finding process to determine the facts of a security incident.
l. Loss: The inability to physically locate or account for classified information.
m. Security Incident: An incident resulting from the mishandling of classified information.
n. Suspected Compromise: A situation where it cannot be determined with certainty that no loss or compromise occurred.

6. Contractor Access to Department of the Air Force Installations (DAF Part 42)

a. General Access and Identification
    i. The Contractor must obtain base identification and vehicle passes, if required, for all Contractor personnel who make frequent visits to or perform work on the Department of the Air Force installation(s) cited in the contract. Contractor personnel are required to wear or prominently display installation identification badges or Contractor-furnished identification badges at all times while visiting or performing work on the installation.
b. Application and Credentialing Process
    i. To obtain base access credentials, the Contractor must submit a written request on company letterhead to the Contracting Officer (CO).
        1. Request Contents: The letter must list the contract number, location of the work site, start and stop dates, and the names of all employees and subcontractor employees requiring access. The

letter must also specify the individual(s) authorized to sign requests for base identification credentials or vehicle passes.

2. Routing: The CO will endorse the request and forward it to the issuing base pass and registration office or Security Forces for processing.
3. Required Documentation: When reporting to the registration office, the authorized Contractor individual(s) must provide the following:
    a. A valid driver's license that complies with the REAL ID Act of 2005
    b. Current vehicle registration
    c. Valid vehicle insurance certificate

c. Controlled and Restricted Area Entry
    i. When work under this contract requires unescorted entry to controlled or restricted areas, the Contractor must comply with the following additional security protocols:
        1. Contact MSgt Maria Dezotell at maria.dezotell@us.af.mil or 701-723-1300 for base access instructions.

d. Emergency Mass Notification System (EMNS)
    i. The Contractor must provide an after-hours contact number or after-hours email in the EMNS for each of their personnel whose normal place of duty is on a DoD installation or within a DoD facility.
        1. Reporting Requirements: The Contractor must comply with any additional requirements in DAFMAN 10-206 for emergency operational reporting.
        2. System Updates: To update information, personnel can access the globe icon on their system desktop screens and choose the "Access Self-Service" option.
        3. Foreign Nationals: Foreign Nationals may participate in the system and may remove themselves from the EMNS at any time.

e. Credential Maintenance and Return Requirements
During the performance of the contract and upon contract closeout, the Contractor is strictly responsible for managing access credentials according to the following requirements:

Event / Change in Status	Required Contractor Action
New Personnel Assigned	Obtain required identification and vehicle passes prior to the employee requiring access to the work site.
Loss of Access Need	Promptly return credentials and vehicle passes for any employee or subcontractor who no longer requires access to the work site.
Pass Expiration	Ensure expired identification passes are immediately returned to the issuing office.

Contract Completion/Termination	Ensure that all base identification and vehicle passes issued to employees and subcontractors are returned to the issuing office.

f. Enforcement
    i. Failure to comply with these base access and credential return requirements may result in the withholding of final payment.

7. Common Access Cards (CAC) for Contractor Personnel (DAF Part 42)

a. CAC Criteria
    i. The Contractor must ensure that all contract and subcontract personnel working at the installations or locations specified in this contract obtain a Common Access Card (CAC) if they meet one or both of the following criteria:
        1. They require logical access to Department of Defense (DoD) computer networks and systems in either the unclassified environment or the classified environment (when authorized by governing security directives).
        2. They perform work that requires the use of a CAC for installation entry control or physical access to facilities and buildings.

b. Application Procedures
    i. The Contractor and its personnel must follow these procedures to obtain CACs:
    ii. The Contractor must provide the Contracting Officer (CO) with a list of personnel who require a CAC. The Government will instruct the Contractor on how to complete the Contractor Verification System (CVS) application and will notify the Contractor upon approval.
    iii. Contractor personnel must obtain a CAC from the nearest Real Time Automated Personnel Identification Documentation System (RAPIDS) Issuing Facility, which is typically the local Military Personnel Flight (MPF).

c. Display of CAC
    i. Contractor personnel must wear or prominently display their CAC while visiting or performing work on Government installations or locations, as required by governing local policy.

d. Ongoing Maintenance and Reporting
    i. During the contract performance period, the Contractor must:
    ii. Provide an updated personnel list to the CO within seven working days of any changes to the list of personnel authorized to have a CAC. The CO will provide this updated list to the authorizing Government official.
    iii. Return CACs in accordance with local policy and directives within seven working days of a change in status for any Contractor personnel who no longer require logical or physical access.
    iv. Return CACs in accordance with local policy and directives within seven working days following a CAC's expiration date.
    v. Report lost or stolen CACs in accordance with local policy and directives.

e. Return Upon Contract Completion

i. Within seven working days following the completion or termination of the contract, the Contractor must return all CACs issued to its personnel to the issuing office or the location specified by local policy and directives.

f. Non-Compliance

i. If the Contractor fails to comply with these requirements, the Government may withhold final payment.