U.S. DEPARTMENT OF JUSTICE
DRUG ENFORCEMENT ADMINISTRATION

Landscaping and Grounds Maintenance

REQUEST FOR QUOTATIONS

RFQ: 15DDHQ26Q00000143

REQUEST FOR QUOTATION
(THIS IS NOT AN ORDER)

THIS RFQ [X] IS [ ] IS NOT A SMALL BUSINESS SET-ASIDE

1. REQUEST NO.	2. DATE ISSUED	3. REQUISITION/PURCHASE REQUEST NO.	4. CERT. FOR NAT. DEF. UNDER BDSA REG. 2 AND/ OR DMS REG. 1	RATING
15DDHQ26Q00000143	06/10/2026	D-26-SG-0069		

5a. ISSUED BY

DEA
Attn: Office of Acquisition (FA)
8701 Morrissette Drive
Springfield, VA 22152-1080

6. DELIVER BY (Date)

7. DELIVERY [ ] FOB DESTINATION [X] OTHER *(See Schedule)*

9. DESTINATION

a. NAME OF CONSIGNEE

b. STREET ADDRESS

c. CITY

d. STATE | e. ZIP CODE

5b. FOR INFORMATION CALL (NO COLLECT CALLS)

NAME	TELEPHONE NUMBER	
	AREA CODE	NUMBER
Jose Marin jose.l.marin@dea.gov		Ext.:

8. TO:

a. NAME | b. COMPANY

c. STREET ADDRESS

d. CITY | e. STATE | f. ZIP CODE

10. PLEASE FURNISH QUOTATIONS TO THE ISSUING OFFICE IN BLOCK 5a ON OR BEFORE CLOSE OF BUSINESS (Date)

IMPORTANT: This is a request for information, and quotations furnished are not offers. If you are unable to quote, please so indicate on this form and return it to the address in Block 5a. This request does not commit the Government to pay any costs incurred in the preparation of the submission of this quotation or to contract for supplies or service. Supplies are of domestic origin unless otherwise indicated by quoter. Any representations and/or certifications attached to this Request for Quotation must be completed by the quoter.

11. SCHEDULE (Include applicable Federal, State and local taxes)

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)
	This is a Request for Quote (RFQ) for Landscape/Grounds Keeping Service See Continuation Sheet(s)				

12. DISCOUNT FOR PROMPT PAYMENT	a. 10 CALENDAR DAYS (%)	b. 20 CALENDAR DAYS (%)	c. 30 CALENDAR DAYS (%)	d. CALENDAR DAYS NUMBER	d. CALENDAR DAYS PERCENTAGE
	0.00 %	0.00 %	0.00 %	0	0.00

NOTE: Additional provisions and representations [ ] are [X] are not attached.

13. NAME AND ADDRESS OF QUOTER

a. NAME OF QUOTER

b. STREET ADDRESS

c. COUNTY

d. CITY | e. STATE | f. ZIP CODE

14. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION

15. DATE OF QUOTATION

16. SIGNER

a. NAME (Type or print)

b. TELEPHONE AREA CODE

c. TITLE (Type or print)

NUMBER

This is a Request for Quotation (RFQ) for Landscaping and Grounds Maintenance. Please see the instructions to Quoter and the product description/specifications attached for more details regarding this requirement. **This procurement is a 100% Small Business set-aside**

All quotes must be on an all or none basis, alternate quotes will not be accepted. All Quoters must submit a complete quotation which will be evaluated based on the criteria listed in Quoter's instruction section. In accordance with FAR Part 12, the Government intends to issue a single firm fixed price purchase order to the eligible, responsible Quoter who presents the best value to the government.

Mandatory Site Visit

A mandatory pre-quotation site visit will be held on June 25, 2026, at the Aviation Operations Center (AOC) Facility located at 2300 Horizon Drive, Fort Worth, TX 76177. Attendance is required for quotation submission. Prospective Quoter's must attend the site visit between 8:00 CST a.m. to 4:00 p.m. CST and sign the attendance sheet. All Quoter's must complete a Facility Access Request Form **(Attachment VII)** and email it to Seungjae.oh@dea.gov. Please submit no later than June 23, 2026, at 1:00 p.m. CST Quotations submitted by Quoter's who did not attend the site visit will be deemed non-responsive and will not be considered. All questions arising from the site visit must be submitted in writing via email by the questions deadline due date. (See Page 20: Section INSTRUCTIONS TO QUOTATIONS)

SCHEDULE OF SUPPLIES/SERVICES

BASE YEAR: 08/01/2026 -07/31/2027				
ITEM #	**DESCRIPTION**	**QTY**	**UNIT PRICE**	**PRICE**
1	**ROUTINE GROUND MANINTENANCE:** Ground Maintenance tasks referenced in the following sections of the Scope of Work: 5.1-Mowing and Raking Areas, 5.4- Weed Control 5.5- Insect and Disease control, 5.7 Mulching, 5.9- Edging Trimming and Pruning, 6- Trash, Litter and Debris Pickup and Removal, 7- Curb Walkway and Sidewalk Maintenance, 8- Entrances, Landing Zones and Paved Areas. Consisting of 29 Occurrences from the last week of April through Last Week of October and 5 Monthly Visits from November through March. For a total of 34 Occurrences.	34	$	$
2	**FERTILIZATION OF LAWNS:** Ground Maintenance tasks referenced in section 5.2 of the Scope of Work. To be performed in the months of April, June and August for a total of 3 occurrences.	3	$	$
3	**SEEDING:** Ground Maintenance Tasks referenced in section 5.3 of the Scope of Work. To be performed annually between the months of January and May. Once Annually.	1	$	$
4	**SODDING AND SOIL:** Ground Maintenance tasks referenced in section 5.6 of the Scope of Work. Price is for Labor and an Estimated allowance of Sod, Soil which may be subject to change according to availability and commercial industry pricing of Sod.	1	$	$
5	**SEASONAL COLOR BEDS:** Ground Maintenance Tasks referenced in section 5.8 of the Scope of Work. To be performed throughout the year.	1	$	$
6	**SPRINKLER AND IRRIGATION SYSTEM MAINTENANCE AND REPAIRS:** Ground Maintenance Tasks referenced in section 9, 9.1, 9.2 of the Scope of Work. Includes winterization of Irrigation System in the last week of October, and Priming/Start-up of system the last week of April.	1	$	$
7	**CONTRACT MANAGEMENT/QA-QC:** Ground Maintenance Tasks referenced in sections 10 and 11 of the Scope of Work. To include scheduling, ordering of materials, coordination, Quality Control and Safety Management.	12	$	$

SCHEDULE OF SUPPLIES/SERVICES

OPTION YR I: 08/01/2027 -07/31/2028				
ITEM #	**DESCRIPTION**	**QTY**	**UNIT PRICE**	**PRICE**
1	**ROUTINE GROUND MANINTENANCE:** Ground Maintenance tasks referenced in the following sections of the Scope of Work: 5.1-Mowing and Raking Areas, 5.4- Weed Control 5.5- Insect and Disease control, 5.7 Mulching, 5.9- Edging Trimming and Pruning, 6- Trash, Litter and Debris Pickup and Removal, 7- Curb Walkway and Sidewalk Maintenance, 8- Entrances, Landing Zones and Paved Areas. Consisting of 29 Occurrences from the last week of April through Last Week of October and 5 Monthly Visits from November through March. For a total of 34 Occurrences.	34	$	$
2	**FERTILIZATION OF LAWNS:** Ground Maintenance tasks referenced in section 5.2 of the Scope of Work. To be performed in the months of April, June and August for a total of 3 occurrences.	3	$	$
3	**SEEDING:** Ground Maintenance Tasks referenced in section 5.3 of the Scope of Work. To be performed annually between the months of January and May. Once Annually.	1	$	$
4	**SODDING AND SOIL:** Ground Maintenance tasks referenced in section 5.6 of the Scope of Work. Price is for Labor and an Estimated allowance of Sod, Soil which may be subject to change according to availability and commercial industry pricing of Sod.	1	$	$
5	**SEASONAL COLOR BEDS:** Ground Maintenance Tasks referenced in section 5.8 of the Scope of Work. To be performed throughout the year.	1	$	$
6	**SPRINKLER AND IRRIGATION SYSTEM MAINTENANCE AND REPAIRS:** Ground Maintenance Tasks referenced in section 9, 9.1, 9.2 of the Scope of Work. Includes winterization of Irrigation System in the last week of October, and Priming/Start-up of system the last week of April.	1	$	$
7	**CONTRACT MANAGEMENT/QA-QC:** Ground Maintenance Tasks referenced in sections 10 and 11 of the Scope of Work. To include scheduling, ordering of materials, coordination, Quality Control and Safety Management.	12	$	$

SCHEDULE OF SUPPLIES/SERVICES

OPTION YR II: 08/01/2028 -07/31/2029				
ITEM #	**DESCRIPTION**	**QTY**	**UNIT PRICE**	**PRICE**
1	**ROUTINE GROUND MANINTENANCE:** Ground Maintenance tasks referenced in the following sections of the Scope of Work: 5.1-Mowing and Raking Areas, 5.4- Weed Control 5.5- Insect and Disease control, 5.7 Mulching, 5.9- Edging Trimming and Pruning, 6- Trash, Litter and Debris Pickup and Removal, 7- Curb Walkway and Sidewalk Maintenance, 8- Entrances, Landing Zones and Paved Areas. Consisting of 29 Occurrences from the last week of April through Last Week of October and 5 Monthly Visits from November through March. For a total of 34 Occurrences.	34	$	$
2	**FERTILIZATION OF LAWNS:** Ground Maintenance tasks referenced in section 5.2 of the Scope of Work. To be performed in the months of April, June and August for a total of 3 occurrences.	3	$	$
3	**SEEDING:** Ground Maintenance Tasks referenced in section 5.3 of the Scope of Work. To be performed annually between the months of January and May. Once Annually.	1	$	$
4	**SODDING AND SOIL:** Ground Maintenance tasks referenced in section 5.6 of the Scope of Work. Price is for Labor and an Estimated allowance of Sod, Soil which may be subject to change according to availability and commercial industry pricing of Sod.	1	$	$
5	**SEASONAL COLOR BEDS:** Ground Maintenance Tasks referenced in section 5.8 of the Scope of Work. To be performed throughout the year.	1	$	$
6	**SPRINKLER AND IRRIGATION SYSTEM MAINTENANCE AND REPAIRS:** Ground Maintenance Tasks referenced in section 9, 9.1, 9.2 of the Scope of Work. Includes winterization of Irrigation System in the last week of October, and Priming/Start-up of system the last week of April.	1	$	$
7	**CONTRACT MANAGEMENT/QA-QC:** Ground Maintenance Tasks referenced in sections 10 and 11 of the Scope of Work. To include scheduling, ordering of materials, coordination, Quality Control and Safety Management.	12	$	$

SCHEDULE OF SUPPLIES/SERVICES

OPTION YR III: 08/01/2029 -07/31/2030				
ITEM #	**DESCRIPTION**	**QTY**	**UNIT PRICE**	**PRICE**
1	**ROUTINE GROUND MANINTENANCE:** Ground Maintenance tasks referenced in the following sections of the Scope of Work: 5.1-Mowing and Raking Areas, 5.4- Weed Control 5.5- Insect and Disease control, 5.7 Mulching, 5.9- Edging Trimming and Pruning, 6- Trash, Litter and Debris Pickup and Removal, 7- Curb Walkway and Sidewalk Maintenance, 8- Entrances, Landing Zones and Paved Areas. Consisting of 29 Occurrences from the last week of April through Last Week of October and 5 Monthly Visits from November through March. For a total of 34 Occurrences.	34	$	$
2	**FERTILIZATION OF LAWNS:** Ground Maintenance tasks referenced in section 5.2 of the Scope of Work. To be performed in the months of April, June and August for a total of 3 occurrences.	3	$	$
3	**SEEDING:** Ground Maintenance Tasks referenced in section 5.3 of the Scope of Work. To be performed annually between the months of January and May. Once Annually.	1	$	$
4	**SODDING AND SOIL:** Ground Maintenance tasks referenced in section 5.6 of the Scope of Work. Price is for Labor and an Estimated allowance of Sod, Soil which may be subject to change according to availability and commercial industry pricing of Sod.	1	$	$
5	**SEASONAL COLOR BEDS:** Ground Maintenance Tasks referenced in section 5.8 of the Scope of Work. To be performed throughout the year.	1	$	$
6	**SPRINKLER AND IRRIGATION SYSTEM MAINTENANCE AND REPAIRS:** Ground Maintenance Tasks referenced in section 9, 9.1, 9.2 of the Scope of Work. Includes winterization of Irrigation System in the last week of October, and Priming/Start-up of system the last week of April.	1	$	$
7	**CONTRACT MANAGEMENT/QA-QC:** Ground Maintenance Tasks referenced in sections 10 and 11 of the Scope of Work. To include scheduling, ordering of materials, coordination, Quality Control and Safety Management.	12	$	$

SCHEDULE OF SUPPLIES/SERVICES

OPTION YR IV: 08/01/2030 -07/31/2031				
ITEM #	**DESCRIPTION**	**QTY**	**UNIT PRICE**	**PRICE**
1	**ROUTINE GROUND MANINTENANCE:** Ground Maintenance tasks referenced in the following sections of the Scope of Work: 5.1-Mowing and Raking Areas, 5.4- Weed Control 5.5- Insect and Disease control, 5.7 Mulching, 5.9- Edging Trimming and Pruning, 6- Trash, Litter and Debris Pickup and Removal, 7- Curb Walkway and Sidewalk Maintenance, 8- Entrances, Landing Zones and Paved Areas. Consisting of 29 Occurrences from the last week of April through Last Week of October and 5 Monthly Visits from November through March. For a total of 34 Occurrences.	34	$	$
2	**FERTILIZATION OF LAWNS:** Ground Maintenance tasks referenced in section 5.2 of the Scope of Work. To be performed in the months of April, June and August for a total of 3 occurrences.	3	$	$
3	**SEEDING:** Ground Maintenance Tasks referenced in section 5.3 of the Scope of Work. To be performed annually between the months of January and May. Once Annually.	1	$	$
4	**SODDING AND SOIL:** Ground Maintenance tasks referenced in section 5.6 of the Scope of Work. Price is for Labor and an Estimated allowance of Sod, Soil which may be subject to change according to availability and commercial industry pricing of Sod.	1	$	$
5	**SEASONAL COLOR BEDS:** Ground Maintenance Tasks referenced in section 5.8 of the Scope of Work. To be performed throughout the year.	1	$	$
6	**SPRINKLER AND IRRIGATION SYSTEM MAINTENANCE AND REPAIRS:** Ground Maintenance Tasks referenced in section 9, 9.1, 9.2 of the Scope of Work. Includes winterization of Irrigation System in the last week of October, and Priming/Start-up of system the last week of April.	1	$	$
7	**CONTRACT MANAGEMENT/QA-QC:** Ground Maintenance Tasks referenced in sections 10 and 11 of the Scope of Work. To include scheduling, ordering of materials, coordination, Quality Control and Safety Management.	12	$	$

STATEMENT OF WORK

CONTRACT DOCUMENTS AND ATTACHMENTS

1. INTRODUCTION

The purpose of this contract is to procure landscaping and grounds maintenance services. Aviation Operations Center (AOC) Facility is located in Fort Worth, Texas.

2. BACKGROUND

The Aviation Division coordinates and over sees operations from the Aviation Operations Center (AOC), which is located at Alliance Airport, Fort Worth, Texas. The property on which the AOC sits consists of 12.3807 acres (539,303 sf) which include approximately 2.66 acres (115,728 sf) of Landscaping Area. The growing season for the Fort Worth, Texas area runs from March through November, however; this can vary from year-to-year based on climate and other environmental factors/changes.

3. SCOPE OF WORK

The contractor must provide the Drug Enforcement Administration (DEA) Aviation Operations Center (AOC) with grounds maintenance services to include but not limited to mowing, edging and trimming, pruning, irrigating, fertilizing, aerating soil, installing new plants, removing plants, replacing and transplanting trees, shrubs and perennial flowers. The Contractor must perform these services in a manner that will promote the growth of healthy grass, trees, shrubs, and plants with a neat and professional appearance. The Contractor must also abide in accordance with the Alliance Airport Association rules and regulations which the AOC is a member. Refer to the ***Attachment (IV)***

4. PERIOD OF PERFORMANCE

One (1) base year and Four (4) option years

POP PERIOD	POP START	POP END
BASE PERIOD	08/01/2026	07/31/2027
OPTION PERIOD I	08/01/2027	07/31/2028
OPTION PERIOD II	08/01/2028	07/31/2029
OPTION PERIOD III	08/01/2029	07/31/2030
OPTION PERIOD IV	08/01/2030	07/31/2031

5. Performance Work Statement Tasks and Critical Subtask:

The contractor must perform the following landscaping maintenance tasks and subtasks to the quality performance and standards addressed or indicated below each task/subtask:

Grounds Maintenance - General Tasks and Requirements:

The Contractor must be responsible for providing management, supervision, labor, material, and equipment required for mowing, irrigating, and cleaning the specified grounds and paved areas. These services shall include: mowing, edging, raking, and trimming grass; irrigating grass, trees, and shrubs; applying fertilizers; weeding; applying poisons/insecticides; seeding grassed areas; maintaining and repairing irrigation sprinkler system; and cleaning up and removing any debris and trash from the worked areas to a landfill that is off the specified property.

The Contractor must perform all work in accordance with all applicable Federal, state, county and municipal laws and regulations. The contractor must perform the following grounds maintenance tasks:

5.1 Mowing & Raking Areas

The grounds must be mowed and raked as needed. Grass must be cut on a weekly basis and maintained from the first week of May through the last week of October (26 Occurrences). During the months of April and November, mowing service must be performed two (2) times per month, Total 34 Occurrences. Work may be rescheduled due to inclement weather conditions or any other unforeseen circumstances that might occur after coordination with a written consent of the COR. The frequency of this service will depend on weather conditions and will not be altered without prior approval of the COR.

The ground includes:

- All the lawns will be mowed to 2½ height and maintained to give a well-manicured appearance
- All debris natural and man-made shall be picked up prior to the mowing of any area
- The contractor shall remove excess clipping turf areas, sidewalks, patios, or other concrete areas.
- Leaf litter and branches on grounds areas shall be cleaned up or raked as needed
- All clippings and debris shall be removed and hauled away to a designated site away from the compound
- Mowing equipment shall be removed from mowing areas at the end of each day and stored at contractor's own facility or location. In no case shall mowing machinery be left on the grounds chained to posts, and etc.
- The contractor shall ensure that the trees, bushes, and other Government owned property that exists on the areas shall not be damaged during the action of mowing. Any damages will be repaired at the contractor's own expense.
- Contractor responsible for monitoring the growth of the grass and schedule cutting/mowing operation as required.

- **Mowing**

The Contractor must mow all grassed areas as needed; grass must be cut to a uniformed height consistent with the best recommended practices for the predominant species of the lawn that meets or exceeds industry standards. Prior to cutting, any trash, paper, or other debris that would detract from the finished

appearance of the cut or present a safety hazard shall be removed. All debris must be disposed by the contractor at an approved location outside facility. Grass cutting is to be accomplished free of scalping, rutting, bruising, and uneven and rough cutting. Cutting must produce a neat, clean, and even cut. Streaks or irregularities, uneven cutting, plowing, or gouging of the soil shall not be permitted. Finished cutting must produce a uniform grass height. Grass clippings must not be windblown or deposited in piles or clumps. Grassed areas, trees, or bushes, which are killed or damaged, must be repaired or replaced. Grass clippings and trimmings generated by cutting must be removed from sidewalks and other paved areas the same day as cutting.

- **Raking**

The contractor must rake all grass and cultivated areas as needed. Raking includes the collection and removal of leaves, pine cones, limbs, and other debris from the raked area. All debris must be disposed of at an approved location outside the compound. Raking must be performed with sufficient frequency so that areas maintain a neat and clean appearance.

5.2 Fertilization of Lawns

Commercial fertilizer must be applied once during the months of April, June, and August. Additional applications may also be required to maintain optimum growth and health of plants. The Rate of application must be per fertilizer manufacturer's directions. Trees and bushes must be fertilized using commercially available fertilizer spikes or water-soluble fertilizer suitable for pressure application. The Rate of application must be according to manufacturer directions. Any change in fertilizer formulation will require approval by the COR. Fertilize all lawn areas as necessary and keep weed free. The Contractor must uniformly apply surface fertilizer to all parcels identified in this solicitation. Fertilizer and spreader must be supplied by the Contractor.

5.3 Seeding

All grassed areas must be re-seeded once a year between January and May using commercially available grass approved by association. It will contain no weeds or other strains of grass. Pre-treatment of these areas with an approved herbicide to remove/kill unwanted weeds and other plant growth must be performed in accordance with the manufacturer's guidelines prior to seeding. The rate of seed application must be according to manufacturer's direction.

- Commercially available industrial standard weed-free topsoil dressing, other than manure, must be applied over all seeded areas immediately after seeding.
- Seeding all grassed areas as necessary and keep weed free.
- The Contractor must uniformly apply surface seeding to all parcels identified in this solicitation. Seeding and spreader shall be supplied by the Contractor.

5.4 Weed Control

Weed control must be applied to vegetation in areas along fences, mulched beds, along sidewalks, parking areas, and the aircraft ramp to prevent the growth of weeds and eradicate any existing weeds. Contractor will remove any visible weeds during the service.

5.5 Insect and Disease Control

Insecticides must be applied by the contractor on a controlled basis under the supervision of a licensed a certified pesticide applicator

- All grounds and vegetation must have an will maintain an environment free of diseases, rodents, insects, and other pests which may damage it.

5.6 Sodding and Soil

The Contractor must install sufficient soil and sod, under all trees and in all median areas in parking lots to cover exposed roots. The Contractor must ensure that sod is healthy and in good condition. The Contractor must maintain or install sufficient soil and sod throughout the year.

5.7 Mulching

The Contractor must install pine bark mulch to all plant and ornamental tree beds. Mulch must be applied to provide a consistent 2" depth to all planting areas and must be replenished throughout the year to maintain this depth. The Contractor must also de-mulch plant beds on an annual basis.

5.8 Seasonal Color Beds

The contractor must provide maintenance and upkeep of the year-round plants in the flowerbeds for the security shack entrance to the facility, main office building entrance and designated smoking areas. Contractor must be responsible for replacement of any dying plant in these flowerbeds when needed.

5.9 Edging, Trimming, and Pruning

All Zones in the compound require mowing, edging, and trimming on a weekly basis, and must be maintained. The Edging & Trimming services are estimated to occur from April through November. Work may be rescheduled due to inclement weather conditions or any other unforeseen circumstances that might occur after coordination with a written consent of the COR. The frequency of this service must depend on weather conditions and will not be altered without prior approval of the COR. All areas must be trimmed in concurrent with mowing. Cutting height must be maintained to two inches in all grass areas. The areas around all trees, bushes, and sprinklers located in the grassed areas must be trimmed at the same height as the mowed grass. All areas bordering these Zones (e.g., curbs, pavements, sidewalks, etc.) must be edged or trimmed. The contractor must provide this service in such a manner as to ensure no damage or erosion to the soil or to existing trees, bushes, sprinklers, drip, or bubblers, and that all clippings, trash and debris are removed from the government premises at the end of the day. Periodic

mowing, edging or trimming may be required from November through March to ensure the neat appearance of the area, but will not be required more than once a month.

- All lawns must be edged to 2 inches in height along sidewalks and other structures.
- All debris must be removed and hauled away to a designated site away from the Government premises.
- A weed-eater may be required where mowing is not feasible.

- **Edging**

The Contractor must edge all sidewalks, driveways, street edges, curbs, other paved areas where cut. Edging must create a clear zone at locations. The edging operation must include removal of grass and other vegetation, which has encroached onto street and other designated surfaces to avoid erosion to the soil and damage to the adjoining grassed areas. All lines must be neat and uniform in appearance. All vegetation growing in the following areas must be removed during the edging operation:

- Sidewalk and driveway expansion joints and cracks.
- Street/driveway curbing expansion joints.
- Cracks between curbing and street/driveway pavement.

Debris generated by edging operations, which falls on or is thrown on sidewalks, on curbs, in gutters, streets, or is thrown on nearby sod, causing an unsightly appearance, shall be removed from the site the day of edging operation and disposal at the approved designated location. Task must be in concurrent with mowing.

- **Trimming**

Grass and weeds must be trimmed around trees, bushes, buildings, fences, poles, posts, fire hydrants, parking lot bumper blocks, boulders, and other fixed obstacles. Trimming height shall match surrounding area grass heights. This task involves all improved grounds as shown in where mowing occurs. All areas must be trimmed concurrent with mowing. Grass clippings and trimmings must be removed from sidewalks and other paved areas the same day as cutting. Damage to trees and bushes from trimming must be repaired by the Contractor. If a plant should die or become unhealthy due to damage, the Contractor will be responsible for replacing the damaged plant with a plant of same size and type. Plant replacement must occur within 15 days of noticed damage.

- **Tree Trimming & Pruning**

All trees must be kept free of dead branches, parasitic, and other unwanted growth at all times. A single pruning of trees may be required when they are dormant (after the first freeze). This must be scheduled by the COR with the Contractor as required. Dead trees must be removed; replacement with like or similar trees at the Contractor's expense. The Contractor must be responsible for the removal of all pruned material from the Government site at the end of the day. Prune all trees along building, structures, and property boundaries.

- Tree and bush pruning are required to keep all pedestrian walkways open, drive ways, security cameras, and any signs free of obstruction.
- All generated clippings and debris shall be removed and hauled away to a designated site outside the compound.
- Minimum safety clearance is at least a ten (10) feet clearance from the ground, three (3) feet clearance from any manmade structure, and clear line of sight for all security cameras. Trees shall be maintained so that there is clear sight at all times.
- Trees must be trimmed and pruned, to include entire tree canopy to allow plenty of sunlight for grass and plant growth and canopy will not be lower than twelve (12) feet, to keep security cameras clear for sight, to maintain a neat and clean appearance.
- Other trees must be pruned on an as required basis to provide safety, clearances and/or to prevent structural damage. Topping and de-horning responsibility must not be permitted.
- Trimming/pruning of trees around utility poles/power lines is the responsibility to notify the COR when trimming/pruning around utility poles/power lines is needed. All clippings and debris must be removed and disposed of at an approved location outside the compound.
- All trimming/pruning removed by the Contractor to an approved off-site facility.
- All pruning should happen in January, thin out and removal any crossing damaged, diseased or dead wood throughout the year.

- **Bush Pruning**

Bushes, small trees, and other vegetation must be maintained according to the Association standard, ***Attachment (IV)*** They must be pruned as required to maintain their natural growth characteristics. All bushes must be pruned on the last Tuesday of every month from April through October. Dead small trees and bushes must be removed; replacement with like or similar trees/ bushes at the Contractor's expense. The Contractor must be responsible for the removal of all pruned material from the Government site at the end of the day. Prune all trees and bushes along building, structures, and property boundaries.

- Bushes and small trees must be trimmed and pruned to enhance the beauty and health of the plant. Hedges must be maintained to their natural mature height and shape.

6. Trash/Litter & Debris Pickup & Removal: *Attachment (III)*

The grounds must have pick-up and removal of litter & debris when needed which includes: Grass Areas, Landscape Rock Areas w/landscape, Roads, Paved Areas, Gravel/Rock Areas w/o landscape, Sidewalk Areas, Loading Dock, and Dumpster Pad. All trash/litter and debris must be removed and hauled to a designated site away from the Government premises.

- The Contractor must collect and dispose of trash, litter and debris in all grassed areas, plant and bush beds, sidewalks, streets and curbs to include other areas in this solicitation such that the areas always have a neat and clean appearance. All trash, litter and debris must be disposed of at an approved location outside the Government premises.

7. Curb, Walkways & Sidewalk Maintenance: *Attachment (III)*

The grounds curbs and walkways shall be blown, swept or maintained by other means as needed so as to keep them free of debris. All debris and moss must be removed and hauled away to a designated site outside the Government premises.

- **Sidewalk Maintenance**

Concrete and asphalt sidewalks must be maintained in an aesthetically pleasing condition by removing all debris as needed.

8. Entrances, Loading Zones, and Paved Areas: *Attachment (III)*

The grounds areas, entrances, loading zones, and paved areas should be blown, swept or maintained by other means as needed so as to keep them free of debris which includes paved Roads, Other Paved Areas, and Loading Dock. All debris and moss must be removed and hauled away to a designated site outside the Government premises.

- All entrances, loading areas, and paved areas must also be inspected on a weekly basis and swept as necessary to maintain a dirt/debris free condition.
- Entrances and Loading Zones must be blown, swept or maintained by other means as needed so as to keep them free of debris.

9. SPRINKLER/IRRIGATION SYSTEM MAINTENANCE AND REPAIRS

The grounds sprinkler/irrigation systems must be maintained as needed which includes; Attachment ***(I and II)***

System	Location	Working Zones
Controller 1	Outside Facility	15 ZONES
Controller 2	Inside Facility	16 ZONES

- The Contractor must repair, at his own expense, all excavations to grounds resulting from sprinkler/irrigation systems, tree/plant removal or other work, returning it to its original condition using clean top soil free of rocks and debris, within one workday following the completion of the work.
- When work is done in grassed areas, contractor must re-sod/re-seed the affected area with the grass approved by association.
- Manual inspections must be conducted once a month if weather permit between the hours of 7:30 a.m. and 4:00 p.m.
- The Contractor must repair all identified defects to components that are available for visual inspection as soon as possible but not later than the next scheduled watering cycles.

- The Contractor must verbally notify the COR of all system defects and failure within 24 hours as well as annotating them on the Quality Control Report Form, which must be turned into the COR at the end of each work day.
- The Contractor must be required to adjust the sprinkler schedule to include spray patterns ensuring optimum water coverage in all areas covered by sprinklers. Within ten (10) working days after award, the Contractor will be given the opportunity to (re)inspect the system and equipment and provide a condition report for all required repairs. The COR will accompany the contractor during this inspection of the system and equipment.

9.1 Sprinkler System Maintenance

The Contractor must inspect the system, to include all components up to and include three-inch pipes, valves and master electrical control unit, and water booster pump during scheduled periods of operation and during a manual operation of the system for those parts of the system not observed during scheduled periods of operation. Any repairs/replacements of parts to system will be done at the Contractors' own expense. Winterizing System the Contractor shall be responsible for winterizing the system and making all necessary adjustments to reactivate the system in the spring.

9.2 Watering Requirements

The Contractor must adjust the sprinkler schedule to include spray patterns ensuring optimum water coverage in all areas covered by sprinklers.

- Sprinklers/Irrigation operations must be conducted according to the schedule unless otherwise specified in writing by the COR.
- All master clocks and their electrical components for the irrigation system of the compound must be maintained in a good working condition on a 24/7 schedule.
- The Contractor must use the Government installed system to accomplish all irrigation at the compound. In the event the Government installed system becomes inoperable, the Contractor shall provide equipment and other means necessary for the irrigation of all areas, with the same acre feet of water as would be provided by the installed sprinkler/irrigation systems.

10. Acceptable Quality Level:

All work described in the statement of work must be complete and visually pleasing, furnish all labor, materials, tools, transportation, services and supplies, or as otherwise stated in this contract, needed to perform all work required to complete the maintenance in a reasonably cost conformity with the specified standards and with commercial standards for Landscaping Maintenance.

The Contractor must provide all labor, equipment, and new materials unless otherwise stated in the Statement of Work. All work, including labor and materials will be guaranteed for a period of one year from the date of acceptance by Aviation Division.

11. Deliverables/Documentation (plans, schedules, and reports)

After award, and no later than ten (10) calendar days prior to the start of the contract, the Contractor must provide the Contracting Officer a projected annual work schedule. The Contracting Officer will have three (3) working days after receipt to review and submit comments/changes to the contractor, who in turn has three (3) working days to provide the Contracting Officer with a written response. The Contractor must also make available to the Contracting Officer, a safety and accident prevention plan within 30 calendar days after award of contract.

- Daily Work Schedule Reports - The COR will issue the Contractor the Quality Control Report Form at ***Attachment V*** the workday prior to the day the work is to be performed. The Contractor must return this form at the end of the workday annotating all work that has been accomplished or any other information that should be aware of. The COR may also use the comment section to annotate any matter regarding contractor performance. Work may be rescheduled due to inclement weather conditions only after coordination with and written consent.
- Must be performed by trained technicians under the direction of an individual who has been certified in the application of such products.
- The Contractor is required to provide proof of insurance within 15 days after award. The required documentation shall be forwarded to the CO through the COR for review and inclusion in the official contract file.
- Within ten (10) days after contract award, the Contractor must provide to the documentation of the certificates of training, licenses, and permits as required for all personnel that will be in contact with pesticides or are performing services that require State, local, or Federal certification, training, or licensing. Required documentation for all new employees shall be provided no later than five (5) calendar days prior to the employees' start work date. The Contractor must insure that all certificates of training, licenses, permits and bonds are kept current and valid.
- The Contractor must provide appropriate signs to mark area that is being work on. Contractor employees shall be required to interrupt their work if necessary to allow foot passage.
- The Contractor must provide proof of coverage with an insurance policy for liability. The policy must maintain minimum coverage of $500,000 to cover any injuries and/or damages that may occur as a result of the performance of this contract.
- The Contractor must have proof and must provide such documentation at the request of the COR that all work is accomplished in accordance with the contract and applicable Federal, State, County, Military, and municipal laws, regulations and/or written directives issued by the Contracting Officer. This documentation must be made available to the Government during the term of the contract. The Contract must comply with the provision of the Federal Insecticide, Fungicide, and Rodenticide Act (7 U.S.C. 136 et seq.) as amended, with the provisions of the Federal Environmental Pesticide Control Act of 1972, Public Law 920516 (86 Stat.973), and all regulations issued thereunder and current EPA, Clean Air Requirements. Only pest control products that have been previously submitted and approved by the will be used.
- The Contractor must issue uniforms and safety equipment for contract employee use. The Contractor must have a maximum of 15 days to ensure that all contract employees wear clothing

that will identify them as employees of the company. A minimum company log attire is required. After the 15 days period, contractor employees who are not so identified by the proper clothing will not be granted access to the compound.

- The Contractor must furnish all equipment, chemicals, fertilizers, repairs, and miscellaneous equipment/materials required for fulfilling the terms and conditions of this contract at its own expense.
- The Contract must submit scanned or electronic images of invoice(s) to the following email address; Invoice.Aviation@dea.gov. Invoices will be sent after service period. The date of record for invoice receipt is established on the day of receipt of the email if it arrives before the end of standard business hours (5:00 p.m. local) or the next business day if the invoice arrives outside of normal business hours. Scanned documents with original signatures in .pdf or other graphic formats attached to the email are acceptable. Digital/electronic signatures and certificates cannot be processed by DEA and shall be returned. In addition to the items required in FAR clause 52.232-25. PROMPT PAYMENT. at (a)(3)(i) through (x). a proper invoice shall also include the following minimum additional information and/or attached documentation.
- Total/cumulative charges for the billing period for each Contract Line Item Number (CLIN);
- Dates upon which items/services were delivered;
- The Contractor's Taxpayer Identification Number (TIN); and
- The Contractor must be registered in the System for Award Management (SAM) database to receive payment from a Government contract. Registration may be accomplished through www.sam.gov or Federal Service Desk (FSD) at www.fsd.gov or by calling 866-606-8220. Tax Identification Numbers shall be annotated on all invoices provided to the Government.
- Contractor will maintain a valid UEI (sam.gov) for duration of contract.

12. Inspection of Grounds Maintenance

Work not meeting contract requirements will cause the Contractor to:

- Rework at no cost to the Government.

13. Hours / Sign In / Holiday Schedule:

- All Contractor employees must sign in with the security shack located in the entrance of facility prior to beginning work and sign out at the end of the workday.
- Scheduled Hours of Operation - The contractor must maintain the following scheduled hours of operations Monday through Friday, 7:30 a.m. to 4:00pm Occasionally, work may be required after the hours of operations.
- The Contractor must establish a standard holiday schedule that coincides with the Government's schedule.
- Unscheduled Government Closings - There are certain types of irregularly occurring circumstances that may prompt the Government to close the office where contractor personnel are working, either on a national or local basis. Examples of such situations are; inclement weather (usually snow) or Agency-declared administrative leave (such as Christmas Eve). When such

situations occur, the Contractor may bill the Government for only the actual hours worked up to the time of the official closing.

14. Security Requirements:

All contractor personnel supporting this procurement are entrusted with a certain level of trust due to the nature of DEA's mission. The Government expects the vendor will employ persons of integrity and trustworthiness. To ensure this, DEA reserves the right to conduct background screening or a full background investigation on all employees if a need arises. While all services provided on this contract will be performed outside of DEA, all contractors must be escorted if the need arises to enter a DEA facility. DEA reserves the right to modify the security requirements found in this contract at any time.

- Contractors shall submit a facility access request form for all personnel performing under this contract no later than (5) five days of contract award prior to the commencement of work
- Every 6 month all the contractors must be renewal facility access.

15. Contract Office Representative (COR)

The COR is responsible for receiving all deliverables, inspecting and accepting the supplies or services provided under the order in accordance with the terms and conditions of this contract. The COR also certifies any invoices/vouchers for acceptance of the supplies furnished for payment, prior to forwarding the original invoice to the payment office. The COR does not have the authority to alter the Contractor's obligations under the contract, or to modify any of the expressed terms, conditions, descriptions, or costs of the agreement. Any contractual alterations/changes to the contract shall be accomplished by the Contracting Officer only and shall be issued in writing and signed by same. The assigned COR will be assigned at time of contract award.

INSTRUCTIONS TO QUOTERS

Questions Deadline/Due Date: Questions in regard to the RFQ are to be submitted to Jose Marin, Contract Specialist at FACN.Proposal.Submission@dea.gov no later than **July 02, 2026, at 9:00 AM EST.** The Government will respond using a Q&A method via an amendment to the solicitation.

Quotation submittal: Quotation must be submitted electronically to Jose Marin, Contract Specialist at FACN.Proposal.Submission@dea.gov on or before **July 15, 2026, at 9:00 AM EST.** Submittal must be on the Quoter's letterhead clearly labeled with company name, address, phone number, point of contact(s) and email address(s). Be advised that late quotations will not be considered. Please note the RFQ number in the subject line of the electronic (email) submission. The quoter must provide an quote acceptance period of 45 days.

Business Information to be Furnished

The quoter must provide the following business information with their business quotation:

- Company Name, Address, Point of Contact
- UEI number
- CAGE CODE number
- Business Classification/Size
- NAICS Code
- Completion of DEA-2852.209-70 – Organizational Conflicts of Interest –The quoter shall refer to clause DEA-2852.209-70 Organizational Conflicts of Interest (MAY 2012) located in attached clause matrix.
- Any changes or updates to the representations and certifications on file in the System for Award Management as required by paragraph (b) of Federal Acquisition Regulation provision 52.212-3 quoter Representations and Certifications – Commercial Items.
- Completion of DEA-2852.242-74 – Contract Administration Points of Contact.
- Price Quotation – Quoter's shall complete the Pricing worksheets **(Attachment VIII)**.
- Failure to provide pricing for all CLINS may result in elimination from further consideration.

The Government may reject all quotes received in response to this solicitation, if doing so is in the best interest of the Government. No telephone or fax requests shall be accepted. This solicitation does not commit the Government to pay any costs incurred in the submission of a quotation.

COMPLIANCE WITH INSTRUCTIONS

The Government will complete a compliance review of all Quoter's submissions, and the DEA will also consider compliance with the instruction of the RFQ. The Government will consider a contractor's noncompliance with these instructions, or any attempt to evade the requirements

imposed by these instructions, as indicative of the conduct the Government may expect from the quoter during performance. The Government also reserves the right to treat noncompliance with these instructions as a risk and may treat such risk as grounds to eliminate any quoter from award consideration.

QUOTATION FORMAT/PAGE LIMITATIONS

Quotes must contain two separate volumes: [i.e. Volume 1: Technical Specification and Volume 2: Business/Price Quotation].

	TITLE	PAGE LIMITATION
VOLUME 1	Executive Summary	25 Pages
	Technical Specification	
VOLUME 2	Business/Price Quotation	No Pages Limit

Paper, Page Size and Markings: Each volume must have a Table of Contents for easy reference. The quotations must be formatted such that, if printed, they fit within 8 ½ x 11- inch paper, in a commercially standard font size (no smaller than 11-point). The Quoter should mark its RFQ response with any proprietary marking, if needed, based on their assessment of the contents of each volume.

Page Limitation. The Quoter (Volumes 1 and 2) must not exceed 25 pages. Quotations must be written in plain English, in a concise, easy to read manner. Note, title page, table of contents, index, and/or glossary shall NOT be counted in the page count limitation. Pages submitted in excess of the page limitations described above will not be evaluated.

Evaluation. The Government will award a contract resulting from this solicitation to the responsible Quoter whose quote, conforming to the solicitation, represents the best value to the Government, price, and other factors considered.

Technical and past performance, when combined, are more important when compared to price.

The following factors shall be used to evaluate quotes; all factors are of in importance in descending order as shown below:

- Factor 1: Corporate Capability
- Factor 2: Technical Approach/Understanding of the Requirement
- Factor 3: Staffing Approach
- Factor 4: Past performance
- Factor 5: Price

Evaluation Factors

Factor 1: Corporate Capability

The Government will evaluate its level of confidence that the quoter has demonstrated an understanding of the scope, complexity, and performance expectations outlined in the Statement of Work (SOW) for Firm Fixed Price landscaping services.

At a minimum, the quote must include:

- Staffing Qualifications: Resumes of key personnel, including supervisors and crew leads, who will be directly involved in performing the landscaping services. Resumes must demonstrate relevant experience, certifications (if any), and technical capabilities related to grounds maintenance, equipment operation, and site supervision.

- Equipment List: A detailed list of landscaping equipment (e.g., mowers, trimmers, blowers, utility vehicles) proposed for use under the contract. The equipment must be suitable, functional, and sufficient to meet the service requirements efficiently.

All technical documents, including spreadsheets, must be formatted to print on standard 8.5" x 11" paper with appropriate page breaks. The total technical submission shall not exceed two (2) pages.

Note: The technical evaluation will focus on the Quoter's ability to demonstrate sufficient personnel qualifications and equipment readiness to ensure successful performance under a Firm-Fixed Price arrangement.

Factor 2: Technical Approach/Understanding of the Requirement

The Government will evaluate its level of confidence that the quoter has demonstrated a technical understanding of the requirement, the approach, and the techniques necessary to satisfy the elements of the Statement of Work. Specifically, the Quoter must clearly demonstrate a well-defined technical approach to accomplishing the Landscaping and Ground Maintenance services to be performed. This includes showcasing its capability to efficiently organize and manage project personnel and resources, ensuring that all tasks are executed in a timely and professional manner consistent with the project's objectives and quality standards.

The Government will assess its level of confidence that the quoter has demonstrated its ability to anticipate risks and ensure quality of services provided based on prior experiences. Examples should show methods for providing, monitoring, and evaluating services with similar requirements and correcting any issues.

Factor 3: Staffing Approach

The Government will evaluate its level of confidence that the quoter demonstrated the ability to recruit qualified candidates who can effectively provide Landscaping services as specified in the Statement of Work. This assessment will consider the contractor's proven track record, recruitment strategies, and success in sourcing candidates with the necessary skills and qualifications to meet the service requirements outlined. The evaluation aims to ensure that the quoter can reliably fulfill the landscaping needs in accordance with the agreed standards and expectations.

Staffing Qualifications: Resumes of all key personnel who will be directly involved in delivering the landscaping services. This includes supervisors, crew leaders, and any other critical team members. The resumes should demonstrate each individual's relevant experience in the landscaping and grounds maintenance industry. This includes prior roles and responsibilities that highlight their expertise in managing landscaping projects, maintaining grounds, and overseeing crews.

Factor 4: Past Performance

The Quoter will be evaluated on their performance under existing and prior contracts for similar services within the last three years based on information obtained from references provided by the Quoter's Past performance based on the level of confidence using Low, Medium, or High risk rating.

The Government will evaluate two (2) contracts or task orders, performed during the past three (3) years that are representative of the Quoter’s capability to provide services with similar scope, magnitude/size, and complexity of past performance, similar to that stated in the Statement of Work.

The Government will supplement the information provided by the Quoter with information the Government obtains through reference checks, contacting the point of contact of the reference checks, its own knowledge/experience, and/or from other sources. These sources may include, but are not necessarily limited to, other Government contracting offices, the Contractor Performance Assessment Reporting System (CPARS), and the Past Performance Information Retrieval System (PPIRS).

Factor 5: Price

Prices will be evaluated for fairness and reasonableness through a price analysis that compares the prices offered against each other and the independent Government estimate. Award shall not be made to an Quoter’s quotation for goods or services that is found to be unbalanced and/or unreasonably low or high.

Options. The Government will evaluate quotes for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an quote is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

Pricing sheet. The Quoter(s) shall complete the Pricing Template **(Attachment VIII)** in accordance with the "Schedule of Supplies/Services" of the RFQ.

Basis for Award.

The Government will award the contract to the responsive and responsible Quoter whose quotation is deemed most advantageous to the Government, considering both price and other relevant factors. Quotations will be evaluated based on the technical criteria outlined in this solicitation and the cost/price submitted.

All technical factors 1-3 will be evaluated using adjectival ratings of High Confidence, Some Confidence, and Low Confidence.

HIGH CONFIDENCE	The Government has ***HIGH CONFIDENCE*** that the Quoter understands the requirement, proposes a sound approach, and will be successful in performing the contract with little or no Government intervention.
SOME CONFIDENCE	The Government has ***SOME CONFIDENCE*** that the Quoter understands the requirement, proposes a sound approach, and will be successful in performing the contract with some Government intervention.
LOW CONFIDENCE	The Government has ***LOW CONFIDENCE*** that the Quoter understands the requirement, proposes a sound approach, or will be successful in performing the contract even with Government intervention.

Past Performance will receive an overall risk rating of Low, Medium, or High; a High-risk rating is considered Unacceptable.

Low Risk	Has little potential to cause disruption of schedule, increased cost or degradation or performance. Normal quoter effort and normal Government monitoring will likely be able to overcome any difficulties.
Medium Risk	Can potentially cause disruption of schedule, increased cost or degradation of performance. Special quoter emphasis and close Government monitoring will likely be able to overcome difficulties.
High Risk	Is likely to cause significant disruption of schedule, increased cost of degradation of performance. Is unlikely to overcome any difficulties, even with special quoter emphasis and close Government monitoring.

The Quoter's proposed cost/price will be assessed separately from the technical factors and will not receive a specific confidence rating.

All evaluation factors other than cost/price, when combined, are significantly more important than cost or price. As technical differences narrow, cost/price will become more important. If there are no significant technical differences, cost/price may be the determining factor for source selection. This is a best-value procurement. The Government may or may not award to the lowest-priced Quoter or the highest technically rated Quote.

ATTACHMENTS:

Attachment I and II - Sprinkler Controller Schedule
Attachment III - AOC MAP
Attachment IV - Alliance Airport Association Rules
Attachment V - Quality Control Report Form
Attachment VI - Performance Requirement Summary
Attachment VII - Facility Access Request Form
Attachment VIII - Pricing Worksheet

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES
Updated through FAC 2026-01

SOLICITATION #: 15DDHQ26Q00000143

52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this address: https://www.acquisition.gov/far-smart-matrix.

(End of provision)

CONTRACTING OFFICER: Check the corresponding box for the provisions and clauses applicable to this procurement.

☐ **52.204-6 UNIQUE ENTITY IDENTIFIER (OCT 2016)**

☐ **52.204-7 SYSTEM FOR AWARD MANAGEMENT (NOV 2024)**

☐ **52.204-7 ALT I SYSTEM FOR AWARD MANAGEMENT (NOV 2024) WITH ALTERNATE I (OCT 2018)**

☒ **52.204-16 COMMERCIAL AND GOVERNMENT ENTITY CODE REPORTING (AUG 2020)**

☐ **52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (OCT 2018)**

☐ **52.209-12 CERTIFICATION REGARDING TAX MATTERS (OCT 2025)**

☐ **52.211-6 BRAND NAME OR EQUAL (AUG 1999)**

☒ **52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (Sep 2023)**

☐ **52.212-2 EVALUATION—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (NOV 2021)**

(a) The Government will award a contract resulting from this solicitation to the responsible offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate offers:

[*Contracting Officer shall insert the significant evaluation factors, such as (i) technical capability of the item offered to meet the Government requirement; (ii) price; (iii) past performance (see FAR 15.304); and include them in the relative order of importance of the evaluation factors, such as in descending order of importance.*]

Technical and past performance, when combined, are [*Contracting Officer state, in accordance with FAR 15.304, the relative importance of all other evaluation factors, when combined, when compared to price.*]

(b) Options. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

(End of provision)

☐ **52.225-7 WAIVER OF BUY AMERICAN STATUTE FOR CIVIL AIRCRAFT AND RELATED ARTICLES (FEB 2016)**

☒ **DOJ-06 NATIONAL SECURITY RISK ASSESSMENT (APR 2014)**

(a) Any offeror responding to this solicitation acknowledges that before acquiring information technology equipment or software, the U.S. Department of Justice and its component entities will assess the supply chain risk of cyber-espionage or sabotage associated with the acquisition of such equipment or software, including any risk associated with such equipment or software being produced, manufactured, or assembled by one or more entities identified as posing a cyber-threat, including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China.

(b) By submitting an offer to this solicitation, the Offeror understands and agrees that the Government retains the right to reject any offer or response to this solicitation made by the Offeror, without any further recourse by, or explanation to, the Offeror, if the Government determines the Offeror or the equipment or software offered by the Offeror, in whole or in part, presents an unacceptable risk to national security.

(c) To assist the Government in assessing whether the acquisition poses a national security risk, offerors are required to complete and submit with its offer or quotation the National Security Acquisition Risk Assessment Questions, which are attached to this solicitation. Offerors must answer all questions completely and accurately to the best of their knowledge and belief. All answers are to be reflective of the parent and subsidiary levels of an organization.

(d) Offerors are also required to request, collect, and forward with its offer or quotation completed National Security Acquisition Risk Assessment Questions from all subcontractors that will provide any equipment or software in performance of the contract or order. Offerors are responsible for the thoroughness and completeness of each subcontractor's submission.

(e) Failure to provide any such requested information may render a proposal unacceptable.

(End of provision)

☐ **JAR 2852.233-70 PROTESTS FILED DIRECTLY WITH THE DEPARTMENT OF JUSTICE (NOV 2020)**

(a) The following definitions apply in this provision:

(1) ''Agency Protest Official'' (APO) means the Deciding Official for a procurement protest filed with a contracting activity of DOJ when the contracting officer will not be the Deciding Official because of the protestor's election under JAR 2833.103(b).

(2) ''Deciding Official'' means the official who will review and decide a procurement protest filed with the agency. The Deciding Official will be the contracting officer unless the protestor requests pursuant to JAR 2833.103(b) that the protest be decided by an individual above the level of the contracting officer, in which case the HCA will designate an APO to serve as the Deciding Official.

(3) ''Interested Party'' means an actual or prospective offeror whose direct economic interest would be affected by the award of a contract or by the failure to award a contract.

(b) Only interested parties may file a protest.

(c) An interested party filing a protest with the DOJ has the choice of requesting either that the Contracting Officer or the APO decide the protest.

(d) A protest filed directly with the DOJ shall:

(1) Indicate that it is a protest to DOJ.

(2) Be filed with the Contracting Officer.

(3) State whether the protestor chooses to have the Contracting Officer or the Agency Protest Official decide the protest. If the protestor is silent on this matter, the Contracting Officer will decide the protest.

(4) Indicate whether the protestor prefers to make an oral or written presentation of arguments in support of the protest to the deciding official.

(5) Include the information required by FAR 33.103(d)(2):

(i) Name, address, facsimile number and telephone number of the protestor.

(ii) Solicitation or contract number.

(iii) Detailed statement of the legal and factual grounds for the protest, to include a description of resulting prejudice to the protestor.

(iv) Copies of relevant documents.

(v) Request for a ruling by the agency.

(vi) Statement as to the form of relief requested.

(vii) All information establishing that the protestor is an interested party for the purpose of filing a protest.

(viii) All information establishing the timeliness of the protest.

(e) The decision by the APO is an alternative to a decision by the Contracting Officer. The APO will not consider appeals from the Contracting Officer's decision on an agency protest and a decision by the APO is final and not appealable.

(f) The Deciding Official may conduct a scheduling conference. The scheduling conference, if conducted, will establish deadlines for oral or written arguments in support of the agency protest and for agency officials to present information in response to the protest issues. The deciding official may hear oral arguments in support of the agency protest at the same time as the scheduling conference, depending on availability of the necessary parties.

(g) Oral conferences may take place either by telephone or in person.

(h) The protestor has only one opportunity to support or explain the substance of its protest. DOJ procedures do not provide for any discovery. The deciding official may request additional information from the agency or the protestor. The deciding official will resolve the protest through informal presentations or meetings to the maximum extent practicable.

(i) A protestor may represent itself or be represented by legal counsel. The DOJ will not reimburse the protester for any legal fees related to the agency protest.

(j) The DOJ will stay award or suspend contract performance in accordance with FAR 33.103(f), unless the contract award is justified, in writing, for urgent and compelling reasons or is determined, in writing, to be in the best interest of the Government. The justification or determination shall be approved at a level above the Contracting Officer. The stay or suspension, unless over-ridden, remains in effect until the protest is decided, dismissed, or withdrawn.

(k) The deciding official will make a best effort to issue a decision on the protest within thirty-five (35) days after the filing date. The decision shall be written, and provided to the protestor using a method that provides for evidence of receipt.

(l) The DOJ may dismiss or stay proceedings on an agency protest if a protest on the same or similar basis is filed with a forum outside DOJ.

(End of Clause)

CONTINUED ON NEXT PAGE

SOLICITATION #:15DDHQ26Q00000143

OFFERORS – COMPLETE THE REPRESENTATIONS BELOW AND RETURN THEM WITH YOUR OFFER OR QUOTE IF THE VERSIONS OF THESE PROVISIONS IN YOUR ANNUAL REPRESENTATIONS AND CERTIFICATIONS IN THE SYSTEM FOR AWARD MANAGEMENT ARE EARLIER THAN OCT 2020.

☒ **52.204-24 REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021)**

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in paragraph (c)(1) in the provision at 52.204-26, Covered Telecommunications Equipment or Services—Representation, or in paragraph (v)(2)(i) of the provision at 52.212-3, Offeror Representations and Certifications-Commercial Products and Commercial Services. The Offeror shall not complete the representation in paragraph (d)(2) of this provision if the Offeror has represented that it "does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services" in paragraph (c)(2) of the provision at 52.204-26, or in paragraph (v)(2)(ii) of the provision at 52.212-3.

(a) *Definitions.* As used in this provision—

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Prohibition.*

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(d) *Representation.* The Offeror represents that—

(1) It ☐ will, ☐ will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

It ☐ does, ☐ does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) *Disclosures.*

(1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(End of provision)

☒ **52.212-3 OFFEROR REPRESENTATIONS AND CERTIFICATIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (OCT 2025)**

Attention is drawn to paragraph (b) of provision 52.212-3, which requests offeror-provided fill-in information in (b)(2), when applicable:

(b)(1) *Annual Representations and Certifications*. Any changes provided by the Offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications in SAM.

(2) The offeror has completed the annual representations and certifications electronically in SAM accessed through http://www.sam.gov. After reviewing SAM information, the Offeror verifies by submission of this offer that the representations and certifications currently posted electronically at FAR 52.212-3, Offeror Representations and Certifications—Commercial Products and Commercial Services, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), at the time this offer is submitted and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs _____.

[*Offeror to identify the applicable paragraphs at (c) through (u) of this provision that the offeror has completed for the purposes of this solicitation only, if any. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer. Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted electronically on SAM.*]

******* Paragraph (i) Contracting Officer fill-in information:** *Paragraph (i)(1): The end products being acquired under this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor are listed by Schedule of Supplies/Services Item Number as follows:* ***[when applicable, enter item numbers with country of origin in parentheses and separated by commas]***

******* Paragraph (k) Contracting Officer fill-in information: select applicable item when an exemption to the Service Contract Labor Standards statute applies.**
☐ **Paragraph k(1) is applicable.** ☐ **Paragraph k(2) is applicable.**
****

(v) (2) The Offeror represents that—

(i) It ☐ does, ☐ does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(ii) After conducting a *reasonable inquiry** for purposes of this representation, that it ☐ does, ☐ does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

* *Reasonable inquiry* has the meaning provided in the clause 52.204–25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

CONTINUED ON NEXT PAGE

SOLICITATION #: 15DDHQ26Q00000143

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: https://www.acquisition.gov/far-smart-matrix.

(End of clause)

		CONTRACTING OFFICER: Check the appropriate box only for clauses that are applicable to this procurement.
☐	52.203-16	**PREVENTING PERSONAL CONFLICTS OF INTEREST (JUN 2020)**
☐	52.203-17	**CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (NOV 2023)**
☐	52.204-9	**PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (JAN 2011)**
☐	52.204-12	**UNIQUE ENTITY IDENTIFIER MAINTENANCE (OCT 2016)**
☒	52.204-13	**SYSTEM FOR AWARD MANAGEMENT MAINTENANCE (OCT 2018)**
☐	52.204-18	**COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE (AUG 2020)**
☒	52.204-19	**INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS (DEC 2014)**
☐	52.204-21	**BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (NOV 2021)**
☒	52.204-23	**PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES, IN ALL SOLICITATIONS AND CONTRACTS (DEC 2023)**
☒	52.204-25	**PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021)**
☒	52.204–27	**PROHIBITION ON A BYTEDANCE COVERED APPLICATION (JUN 2023)**

(a) Definitions. As used in this clause—

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

Information technology, as defined in 40 U.S.C. 11101(6)—

(1) Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(i) Of that equipment; or

(ii) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(2) Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but

(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

(b) Prohibition. Section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328), the No TikTok on Government Devices Act, and its implementing guidance under Office of Management and Budget (OMB) Memorandum M-23-13, dated February 27, 2023, "No TikTok on Government Devices" Implementation Guidance, collectively prohibit the presence or use of a covered application on executive agency information technology, including certain equipment used by Federal contractors. The Contractor is prohibited from having or using a covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor's employees; however, this prohibition does not apply if the Contracting Officer provides written notification to the Contractor that an exception has been granted in accordance with OMB Memorandum M-23-13.

(c) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for the acquisition of commercial products or commercial services.

(End of clause)

☐	52.207-5	**OPTION TO PURCHASE EQUIPMENT (FEB 1995)**
☒	52.212-4	**CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (NOV 2023)**
☐	52.212-4 ALT I	**CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (NOV 2023) WITH ALTERNATE I (NOV 2021)**

☒ **JAR 2852.212-4 TERMS AND CONDITIONS—COMMERCIAL ITEMS (NOV 2020) (DEVIATION)**

When a commercial item is contemplated (using FAR part 12 procedures or otherwise) and the contract will include FAR 52.212–4, the following replaces subparagraph (g)(2); paragraph (h); subparagraph (i)(2); paragraph (s); and paragraph (u), Unauthorized Obligations, of the basic FAR clause, and adds paragraph (w), as follows:

(g)(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment act regulations at 5 CFR part 1315, as modified by subparagraph (i)(2), *Prompt payment,* of this clause.

* * * * *

(h) *Patent indemnity.* Contractor shall indemnify and hold harmless the Government and its respective affiliates, officers, directors, employees, agents, successors and assigns (collectively, ''Indemnities'') from and against any and all liability and losses incurred by the Indemnities that are (i) included in any settlement and/or (ii) awarded by a court of competent jurisdiction arising from or in connection with any third party claim of infringement made against Indemnities asserting that any product or service supplied under this contract constitutes infringement of any patent, copyright, trademark, service mark, trade name or other proprietary or intellectual right. This indemnity shall not apply unless Contractor shall have been informed within a reasonable time by the Government of the claim or action alleging such infringement and shall have been given such opportunity as is afforded by applicable laws, rules, or regulations to participate in its defense. This indemnity also shall not apply to any claim unreasonably settled by the Government which obligates Contractor to make any admission or pay any amount without written consent signed by an authorized officer of Contractor, unless required by final decree of a court of competent jurisdiction.

* * * * *

(i)(2) *Prompt payment.* The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations (5 CFR part 1315), with the following modification regarding the due date: For the sole purpose of computing an interest penalty due the Contractor, the Government agrees to inspect and determine the acceptability of any supply delivered or service performed specified in the invoice within thirty (30) days of receipt of a proper invoice from the Contractor, after which time, if no affirmative action has been taken by the Government to accept such supply or service, the supply or service will be deemed accepted and payment due thirty (30) days from the date of deemed acceptance. If the Government makes the determination that the item delivered or service performed is deficient or otherwise unacceptable, or the invoice is otherwise determined not to be a proper invoice, the terms and conditions of this paragraph regarding prompt payment will apply to the date the Contractor corrects the deficiency in the item delivered or service performed or submits a proper invoice. If actual acceptance occurs within the constructive acceptance period, the Government will base the determination of an interest penalty on the actual date of acceptance. The constructive acceptance requirement does not, however, compel Government officials to accept supplies or services, perform contract administration functions, or make payment prior to fulfilling their responsibilities.

* * * * *

(s) *Order of precedence.* Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Payments, Invoice, Other Compliances, and Compliance with Laws Unique to Government Contracts provisions of the basic FAR clause at 52.212–4, and the Unauthorized Obligations and Contractor's Commercial Supplier Agreements—Unenforceable Clauses provisions of JAR 2852.212–4.

(3) FAR 52.212–5.

(4) Other paragraphs of the basic FAR clause at 52.212–4, with the exception of paragraph (o), Warranty, and those paragraphs identified in this deviation of 52.212–4.

(5) Addenda to this solicitation, contract, or order, including contractor's Commercial supplier agreements incorporated into the contract.

(6) Solicitation provisions if this is a solicitation.

(7) Paragraph (o), Warranty, of the basic FAR clause at 52.212–4.

(8) The Standard Form 1449.

(9) Other documents, exhibits, and attachments.

(10) The specification.

* * * * *

(u) *Unauthorized obligations.*

(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract or order is subject to any Commercial supplier agreement that includes any language, provision, or clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (see 31 U.S.C. 1341), the following shall govern:

(i) Any such language, provision, or clause is unenforceable against the Government.

(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the commercial supplier agreement. If the commercial supplier agreement is invoked through an ''I agree'' click box or other similar mechanism (*e.g.,* ''clickwrap'' or ''browse-wrap'' agreements), execution does not bind the Government or any Government authorized end user to such clause.

(iii) Any such language, provision, or clause is deemed to be stricken from the commercial supplier agreement and have no effect.

(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

* * * * *

(w) *Commercial supplier agreements—unenforceable clauses.* When any supply or service acquired under this contract or order is subject to a contractor's commercial supplier agreement, the following shall be deemed incorporated into such agreement and modifies and replaces any similar language, provision, or clause in such agreement. As used herein, ''this agreement'' means any contractor commercial supplier agreement:

(1) Notwithstanding any other provision of this agreement, when the end user is an agency or instrumentality of the U.S. Government, the following shall apply:

(i) *Applicability.* This agreement is a part of a contract between commercial supplier and the U.S. Government for the acquisition of the supply or service that necessitates a license or other similar legal instrument (including all contracts, task orders, and delivery orders under FAR part 12).

(ii) *End user.* This agreement shall bind the Government as end user but shall not operate to bind the Government employee or person acting on behalf of the Government in his or her personal capacity.

(iii) *Law and disputes.* This agreement is governed by Federal law.

(A) Any language, provision, or clause purporting to subject the U.S. Government to the laws of any U.S. state, territory, district, or municipality, or the laws of a foreign nation, except where Federal law expressly provides for the application of such laws, is hereby deleted and shall have no effect.

(B) Any language, provision, or clause requiring dispute resolution in a specific forum or venue that is different from that prescribed by applicable Federal law is hereby deleted and shall have no effect.

(C) Any language, provision, or clause prescribing a different time period for bringing an action than that prescribed by applicable Federal law in relation to a dispute is hereby deleted and shall have no effect.

(iv) *Continued performance.* Notwithstanding any other provision in this agreement, if the Contractor believes the Government to be in breach of this contract, order, or agreement, it shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing performance as set forth in subparagraph (d), Disputes, of FAR 52.212–4.

(v) *Arbitration; equitable or injunctive relief.* In the event of a claim or dispute arising under or relating to the contract, order, or this agreement,

(A) binding arbitration shall not be used unless otherwise specifically authorized by agency guidance, and

(B) equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the Government only when explicitly provided by statute.

(vi) *Updating terms.*

(A) After award, the contractor may unilaterally revise terms if they are not material. Material terms are defined as:

(1) Terms that change Government rights or obligations;

(2) Terms that increase Government prices;

(3) Terms that decrease the overall level of service; or

(4) Terms that limit any other Government right addressed elsewhere in this contract.

(B) For revisions that materially change the terms of the contract, the revised commercial supplier agreement must be incorporated into the contract using a bilateral modification.

(C) Any agreement terms or conditions unilaterally revised subsequent to award that are inconsistent with any material term or provisions of this contract shall not be enforceable against the Government, and the Government shall not be deemed to have consented to them.

(vii) *Order of precedence.* Any Order of Precedence clause in any commercial supplier agreement is not enforceable against the Government. The applicable Order of Precedence for this contract, order, or agreement is FAR 52.212–4(s), as revised by JAR 2812.302 and 2852.212–4(s).

(viii) *No automatic renewals.* If any license or service tied to period payment is provided under this agreement (*e.g.,* annual software maintenance or annual lease term), such license or service shall not renew automatically upon expiration of its current term without prior express consent by a properly warranted contracting officer, and any provision or term of any license or service purporting to provide for automatic renewal is unenforceable against the Government.

(ix) *Indemnification by the Government or end-user.* Any language, provision, or clause of this commercial supplier agreement requiring the Government or End-user to indemnify the commercial supplier or licensor is not enforceable against the Government.

(x) *Indemnification by the commercial supplier or licensor.* Any clause of this agreement requiring or permitting the commercial supplier or licensor to defend the Government as a condition of indemnifying the Government for any claim of infringement is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. 516.

(xi) *Audits.* Any language, provision, or clause of this commercial supplier agreement permitting Contractor to audit the end user's compliance with this agreement is not enforceable against the Government. To the extent any language, provision or clause of this agreement permits Contractor to audit the Government's compliance under this contract, order, or agreement, such language, provision, or clause of this agreement is hereby stricken and replaced as follows:

''(A) If Contractor reasonably believes that the Government has violated the terms of this agreement with regard to the restrictions on authorized use and/or the number of authorized users, upon written request from Contractor, including an explanation of the basis for the request, DOJ will provide a redacted version of the Government's most recent Security Assessment and Authorization package (SAA) to Contractor on a confidential basis, so that Contractor may reasonably verify the Government's compliance with its obligations under this agreement. Contractor understands and agrees that the Government will remove or redact any information from the SAA that it reasonably believes may compromise (a) the security of the Government's information technology environment; (b) the confidentiality of any third-party proprietary or confidential information; (c) any confidential, sensitive law enforcement information; and (d) any other information that the Government believes may compromise a past, current, or prospective investigation, prosecution, or litigation. Notwithstanding the preceding, and subject to the Government's policies and procedures for such review, including but not limited to complying with all Government security requirements prior to being granted access to the Government's facilities, including the execution of appropriate confidentiality and/or non-disclosure agreements, the Government will arrange, upon Contractor's written request, for Contractor to view an un-redacted version of the SAA on Government premises. Contractor understands that Contractor will be provided a copy of the un-redacted SAA on Government premises only and that no un-redacted copy of the SAA, or any medium containing information relating to it, will be permitted to be removed from Government premises.

(B) The Contractor also understands and agrees that the Contractor shall make a request under this paragraph no more than on an annual basis and only during the period of the contract, and that any activities performed by Contractor under this clause will be performed at Contractor's expense, without reimbursement by the Government.

(C) Discrepancies found with regard to the restrictions on authorized use and/or the number of authorized users may result in a charge by Contractor to the Government. Any resulting invoice must comply with the proper invoicing and payment requirements specified in the contract. This charge, if disputed by the Government, will be resolved through the Disputes clause at 52.212–4(d); no payment obligation shall arise on the part of the Government until the conclusion of the dispute process.''

(xii) *Taxes or surcharges.* Any taxes or surcharges which the Contractor seeks to pass along to the Government as end user will be governed by the terms of the underlying Government contract and, in any event, must be submitted to the Contracting Officer for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the Government contract.

(xiii) *Non-assignment.* This agreement may not be assigned, nor may any rights or obligations thereunder be delegated, without the Government's prior approval, except as expressly permitted under FAR 52.212–4 (b), Assignment.

(xiv) *Confidential information.*

(A) During the term of this contract or order, either party may identify information as ''confidential information,'' and there shall be no disclosure, dissemination, or publication of any such information except to the extent required for the performance of this contract or order and otherwise provided in this clause or by statute or regulation. Specifically, the parties agree that the party receiving confidential information may only disclose such information to its employees and contractors on a ''need-to-know'' basis to carry out the obligations of this contract or order, and that subcontractors performing under this Agreement are subject to the same stipulations provided in this provision. The parties also agree that this provision shall survive the termination of this contract or order, and any confidential information obtained or received which comes within these restrictions shall remain confidential, provided that the obligation to treat information as confidential shall not apply to information which is or becomes publicly available through no improper action of the receiving party; is or comes to be in the receiving party's possession independent of its relationship with the disclosing party; is developed by or becomes known to the receiving party without use of any confidential information of the disclosing party; or is obtained rightfully from a third party not bound by an obligation of confidentiality. Additionally, nothing in this contract or order shall restrict disclosure by the receiving party pursuant to any applicable law, including but not limited to the Freedom of Information Act, 5 U.S.C. 552, *et seq.,* or an order of any court of competent jurisdiction, provided that in either such case the receiving party gives prompt notice to the disclosing party to allow the disclosing party to interpose an objection to such disclosure, take action to assure confidential handling of the confidential information, or take such other action as it deems appropriate to protect its confidential information.

(B) The Government considers and hereby identifies as confidential any and all information related to any inquiries and/or searches performed by the Government or by contractor at the Government's direction under this contract or order, including the subject of any such inquiry or search and any and all search terms, regardless of whether provided in writing or orally to Contractor, and Contractor agrees that it may only disclose such information to its employees and contractors on a ''need-to-know'' basis to carry out the obligations of this contract or order and that it will not share, reveal, divulge, disclose, disseminate, or publicize any such information to any third party except as provided in this provision without the prior written approval of the Contracting Officer. Contractor also understands and agrees that any subcontractors performing under this contract or order are subject to the same stipulations and that Contractor may be held responsible for any violations of confidentiality by a subcontractor.

(C) These provisions are consistent with and do not supersede, conflict with, or otherwise alter an employee's obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by Executive orders and statutory provisions relating to whistleblower protection are incorporated into this contract and are controlling.

(D) The Government may share the terms, conditions and prices set forth in this Order with, and provide a copy of the Order to, other Executive branch agencies of the U.S. Government, provided that the Government shall ensure that other Executive branch agencies to which it provides such information will be required to treat all such information consistent with terms and conditions set forth in this Order.

(E) Notwithstanding anything in this agreement, the Government may retain any confidential information as required by law, regulation, or its internal document retention procedures for legal, regulatory, or compliance purposes; provided, however, that all such retained confidential information will continue to be subject to the confidentiality obligations of this Order.

(xv) *Authorized users.* Authorized users may include full and part-time employees of the Government, including those working at or from remote locations, and contractors and contractor employees working within the scope of their contract with the Government, including those at or from remote locations.

(xvi) *Authorized use.* Authorized users are authorized to use the product or service acquired under this contract in performing business on behalf of the Government. Any information obtained or acquired by the Government under this contract may be used by the Government in the performance of Government business.

(2) If any language, provision, or clause of this agreement conflicts or is inconsistent with the preceding paragraph (w)(1), the language, provisions, or clause of paragraph (w)(1) shall prevails to the extent of such inconsistency.

(End of clause)

☒ **52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (MAR 2026)**

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

(1) 52.203-19, Prohibition on Requiring Certain Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204–23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Dec 2023) (Section 1634 of Pub. L. 115–91).

(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Sec.889(a)(1)(A) of Pub. L. 115-232)

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015) (Executive Order 13658).

(5) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (Mar 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801).

(6) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(7) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004)(Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

[*CONTRACTING OFFICER: CHECK THE CORRESPONDING BOX FOR EACH CLAUSE THAT APPLIES TO THIS ORDER.*]

☐ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Jun 2020), with Alternate I (Nov 2021) (41 U.S.C. 4704 and 10 U.S.C. 4655).

☐ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Nov 2021) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 3509)).

☐ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (June 2010) (Section 1553 of Pub. L. 111-5). (*Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.*)

☐ (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (JUN 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note).

☐ (5) [Reserved]

☐ (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

☐ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

☒ (8) 52.204–27, Prohibition on a ByteDance Covered Application (June 2023) (Section 102 of Division R of Pub. L. 117–328).

☒ (9) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Jan 2025) (31 U.S.C. 6101 note).

☐ (10) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).

☐ (11) [Reserved]

☐ (12) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Oct 2022) (15 U.S.C. 657a).

☐ (13) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2022) (i*f the offeror elects to waive the preference, it shall so indicate in its offer*) (15 U.S.C. 657a).

☐ (14) [Reserved]

☒ (15)(i) 52.219-6, Notice of Total Small Business Set-Aside (NOV 2020) (15 U.S.C. 644).

☐ (ii) Alternate I (Mar 2020).

☐ (16)(i) 52.219-7, Notice of Partial Small Business Set-Aside (NOV 2020) (15 U.S.C. 644).

☐ (ii) Alternate I (Mar 2020) of 52.219-7.

☐ (17) 52.219-8, Utilization of Small Business Concerns (Jan 2025) (15 U.S.C. 637(d)(2) and (3)).

☐ (18)(i) 52.219-9, Small Business Subcontracting Plan (Jan 2025) (15 U.S.C. 637(d)(4)).

☐ (ii) Alternate I (Nov 2016) of 52.219-9.

☐ (iii) Alternate II (Nov 2016) of 52.219-9.

☐ (iv) Alternate III (Jan 2025) of 52.219-9.

☐ (v) Alternate IV (Jan 2025) of 52.219-9.

☐ (19)(i) 52.219-13, Notice of Set-Aside of Orders (Mar 2020) (15 U.S.C. 644(r)).

☐ (ii) Alternate I (Mar 2020) of 52.219-13.

☐ (20) 52.219-14, Limitations on Subcontracting (Oct 2022) (15 U.S.C. 637(a)(14)).

☐ (21) 52.219-16, Liquidated Damages—Subcontracting Plan (Sep 2021) (15 U.S.C. 637(d)(4)(F)(i)).

☐ (22) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Feb 2024) (15 U.S.C. 657 f).

☐ (23)(i) 52.219-28, Post Award Small Business Program Representation (Jan 2025) (15 U.S.C. 632(a)(2)).

☐ (ii) Alternate I (Mar 2020) of 52.219-28.

☐ (24) 52.219-29, Notice of Set-Aside for Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (Oct 2022) (15 U.S.C. 637(m)).

☐ (25) 52.219-30, Notice of Set-Aside for Women-Owned Small Business (WOSB) Concerns Eligible Under the WOSB Program (Oct 2022) (15 U.S.C. 637(m)).

☐ (26) 52.219–32, Orders Issued Directly Under Small Business Reserves (Mar 2020) (15 U.S.C. 644(r)).

☐ (27) 52.219–33, Nonmanufacturer Rule (Sep 2021) (15 U.S.C. 637(a)(17)).

☒ (28) 52.222-3, Convict Labor (Jun 2003) (E.O. 11755).

☒ (29) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Mar 2026) (E.O. 13126).

☐ (30) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

☐ (31)(i) 52.222-26, Equal Opportunity (Sept 2016) (E.O. 11246).

☐ (ii) Alternate I (FEB 1999) of 52.222-26.

☐ (32)(i) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).

☐ (ii) Alternate I (Jul 2014) of 52.222-35.

☐ (33)(i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).

☐ (ii) Alternate I (Jul 2014) of 52.222-36.

☐ (34) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).

☐ (35) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).

☒ (36)(i) 52.222-50, Combating Trafficking in Persons (Oct 2025) (22 U.S.C. chapter 78 and E.O. 13627).

☐ (ii) *Alternate I* (Mar 2015) of 52.222-50 (Nov 2021) (22 U.S.C. chapter 78 and E.O. 13627).

☒ (37) 52.222-54, Employment Eligibility Verification (Jan 2025). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

☐ (38)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA–Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

☐ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

☐ (39) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (May 2024) (E.O. 13693).

☐ (40) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (May 2024) (E.O. 13693).

☐ (41)(i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).

☐ (ii) Alternate I (Oct 2015) of 52.223-13.

☐ (42)(i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (Jun 2014) (E.O. 13423 and 13514).

☐ (ii) Alternate I (Jun 2014) of 52.223-14.

☐ (43) 52.223-15, Energy Efficiency in Energy-Consuming Products (May 2020) (42 U.S.C. 8259b).

☐ (44)(i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (Oct 2015) (E.O. 13423).

☐ (ii) Alternate I (Jun 2014) of 52.223-16.

☐ (46) 52.223-20, Aerosols (May 2024) (E.O. 13693).

☐ (47) 52.223-21, Foams (May 2024) (E.O. 13693).

☐ (48)(i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

☐ (ii) Alternate I (Jan 2017) of 52.224-3.

☐ (49)(i) 52.225-1, Buy American—Supplies (Oct 2022) (41 U.S.C. chapter 83).

☐ (49)(ii) Alternate I (Oct 2022) of 52.225-1.

☐ (50)(i) 52.225-3, Buy American—Free Trade Agreements—Israeli Trade Act (Nov 2023) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43.

☐ (ii) Alternate I (Jan 2021) of 52.225-3.

☐ (iii) Alternate II (Jan 2025) of 52.225-3.

☐ (iv) Alternate III (Feb 2024) of 52.225-3.

☐ (v) Alternate IV (Oct 2022) of 52.225-3.

☐ (51) 52.225-5, Trade Agreements (Nov 2023) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

☐ (52) 52.225-13, Restrictions on Certain Foreign Purchases (Feb 2021) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

☐ (53) 52.225-26, Contractors Performing Private Security Functions Outside of the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).

☐ (54) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

☐ (55) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

☒ (45) 52.226-8, Encouraging Contractor Policies to Ban Text Messaging While Driving (MAY 2024) (E.O. 13513).

☐ (56) 52.229-12, Tax on Certain Foreign Procurements (Feb 2021).

☐ (57) 52.232-29, Terms for Financing of Purchases of Commercial Items (Nov 2021) (41 U.S.C. 4505, 10 U.S.C. 3805).

☐ (58) 52.232-30, Installment Payments for Commercial Items (Nov 2021) (41 U.S.C. 4505, 10 U.S.C. 3805).

☒ (59) 52.232-33, Payment by Electronic Funds Transfer—System for Award Management (Oct 2018) (31 U.S.C. 3332).

☐ (60) 52.232-34, Payment by Electronic Funds Transfer—Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).

☐ (61) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332)

☐ (62) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

☐ (63) 52.242-5, Payments to Small Business Subcontractors (JAN 2017) (15 U.S.C. 637(d)(13)).

☐ (64)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

☐ (ii) Alternate I (Apr 2003) of 52.247-64.

☐ (iii) Alternate II (Nov 2021) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

☐ (1) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).

☐ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67, *et seq*.).

☐ (3) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

☐ (4) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67, *et seq*.).

☐ (5) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (May 2014) (41 U.S.C. chapter 67, *et seq.*).

☐ (6) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (May 2014) (41 U.S.C. chapter 67, *et seq.*).

☐ (7) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022). *(FAC 2022-04)*

☐ (8) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706). *(FAC 2022-04)*

☐ (9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (JUN 2020) (42 U.S.C. 1792).

(d) *Comptroller General Examination of Record*. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records—Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Nov 2021) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 3509)).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.204–23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Nov 2021) (Section 1634 of Pub. L. 115–91).

(iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Sec. 889(a)(1)(A) of Pub. L. 115-232)

(v) 52.204–27, Prohibition on a ByteDance Covered Application (June 2023) (Section 102 of Division R of Pub. L. 117–328).

(vi) 52.219-8, Utilization of Small Business Concerns (Jan 2025) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(vii) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(viii) 52.222-26, Equal Opportunity (Sept 2016) (E.O. 11246).

(ix) 52.222-35, Equal Opportunity for Veterans (JUN 2020) (38 U.S.C. 4212).

(x) 52.222-36, Equal Opportunity for Workers with Disabilities (JUN 2020) (29 U.S.C. 793).

(xi) 52.222-37, Employment Reports on Veterans (JUN 2020) (38 U.S.C. 4212).

(xii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xiii) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).

(xiv) ☒ (A) 52.222-50, Combating Trafficking in Persons (Oct 2025) (22 U.S.C. chapter 78 and E.O. 13627).

☐ (B) Alternate I (Mar 2015) of 52.222-50 (Nov 2021) (22 U.S.C. chapter 78 and E.O. 13627).

(xv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).

(xvi) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).

(xvii) 52.222-54, Employment Eligibility Verification (JAN 2025) (E.O. 12989).

(xviii) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022). *(FAC 2022-04)*

(xix) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706). *(FAC 2022-04)*

(xx)(A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(B) Alternate I (Jan 2017) of 52.224-3.

(xxi) 52.225-26, Contractors Performing Private Security Functions Outside of the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).

(xxii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (JUN 2020) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxiii) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (Mar 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801). Flow down required in accordance with paragraph (c) of 52.232-40.

(xxiv) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial products and commercial services a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

☐ **52.223-2 AFFIRMATIVE PROCUREMENT OF BIOBASED PRODUCTS UNDER SERVICE AND CONSTRUCTION CONTRACTS (MAY 2024)**

*****fill-in information in paragraph (d); enter agency point of contact name, phone #, and e-mail address *****

☐ **52.225-8 DUTY-FREE ENTRY (OCT 2025)**

☐ **52.232-18 AVAILABILITY OF FUNDS (APR 1984)**

☒ **52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)**

☐ **52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (NOV 2020)**

CONTRACTING OFFICER: List additional FAR clauses below, as needed, by entering the clause number, title, and date for each clause added.

52.217-8 Option to Extend Services
52.217-9 Option to Extend the Term of the Contract

The following clauses are also applicable as indicated below.

☒ **DEA-2852.203-70 FORMER EMPLOYMENT OR ASSIGNMENT WITH THE DEA (SEP 2021)**

(a) Any offeror or contractor who intends to employ any individual who either currently works for DEA, or had been employed with DEA as a Federal employee within the previous **five (5) years** for work supporting a prospective or active DEA contract must notify DEA of its intent as described in this clause.

(b) The offeror or contractor shall instruct any prospective or current employee meeting the criteria in paragraph (a), above, to complete and sign a DEA Contractor Ethics Questionnaire. The questionnaire is available for download at https://www.dea.gov/sites/default/files/2020-06/contractor_ethics_questionnaire_jan_2020.pdf. When the intent to employ such individual is known prior to the award of a new contract or order, the contractor shall submit the employee's completed questionnaire and résumé to DEA concurrently with its proposal. When the intent is to employ such individual under an existing contract or order, the contractor shall submit the completed questionnaire and résumé electronically to the cognizant DEA contracting officer **AND** ethicsFAC@usdoj.gov.

(c) The offeror or contractor understands that any such employees described in paragraph (a) are prohibited from appearing before, or communicating with, the Federal Government on behalf of a contractor regarding a Government contract, investigation or other particular matter that they participated in personally and substantially as a Federal employee with the intent to influence Government officials in those matters for the lifetime of those matters.

(d) The offeror or contractor further understands that for two (2) years after leaving the Federal Government, such employees described in paragraph (a) are prohibited from appearing before, or communicating with, the Government with the intent to influence on behalf of a contractor regarding a Government contract, investigation or other particular matter that they did not participate in personally and substantially as a Federal employee, but that was under their official responsibility during their last year in the Government. For purposes of this clause, an employee is defined as one appointed under Title 5, Section 2015 or Title 21, Section 878 of the United States Code.

(e) If DEA determines after reviewing questionnaire responses or conducting other inquiries that the prospective employee is disqualified for assignment to the contract based on an unfavorable suitability and/or security determination, or may violate the post-employment restrictions described in paragraphs (c) or (d), above, or other applicable laws if allowed to work on or support the contract/task order, at DEA's request, the offeror or contractor must not assign such employee to work under a prospective or active contract.

(f) If an offeror or contractor fails to provide a required Questionnaire, the prospective employee will not be approved to work under the DEA contract or order until such time as the Questionnaire is submitted, reviewed, and approved in accordance with established procedures.

(End of clause)

☒ **DEA-2852.209-70 ORGANIZATIONAL CONFLICTS OF INTEREST (SEP 2021)**

(a) The Contractor warrants that, to the best of its knowledge and belief, there are no relevant facts or circumstances that would give rise to an organizational conflict of interest, as defined in FAR Subpart 9.5, or that the Contractor has disclosed all such relevant information.

(b) In the event that an actual, potential, or apparent organizational conflict of interest is discovered after award, the Contractor shall make full disclosure of the particular facts and circumstances to the Contracting Officer in writing. This disclosure shall include a description of the actions that the Contractor has taken, or proposes to take in order to avoid, mitigate, or neutralize the risk to the Government.

(c) Remedies. The Contracting Officer may terminate this contract for convenience, in whole or in part, if deemed necessary to avoid or mitigate an actual or apparent organizational conflict of interest. In the event that the Contractor failed to disclose in a timely manner, or misrepresented the facts and circumstances of, an actual, potential, or apparent organizational conflict of interest of which it had prior knowledge, the Contracting Officer may terminate this contract for default or cause, and pursue additional remedies, including debarment, as may be provided by law.

(d) In the event of repetitive failures to provide this report, the contract may be terminated for default.

(End of clause)

☐ **DEA-2852.211-71 SCHEDULED AND UNSCHEDULED CLOSURES OF GOVERNMENT OFFICES (JUL 2021)**

(a) In accordance with 5 U.S.C. 6103, Federal Government offices are closed for ordinary business in observance of the following holidays:

- New Year's Day
- Birthday of Martin Luther King, Jr.
- Washington's Birthday
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Columbus Day
- Veteran's Day
- Thanksgiving Day

- Christmas Day
- Inauguration Day (*Federal offices in the Washington DC metropolitan area only*)

(b) Federal offices may close at other times without advance notice due to emergencies, inclement weather, interruption of utilities, or other reasons. Such closures may be declared by the President, Office of Personnel Management, Office of Management and Budget, the Administrator of the DEA, or other appropriate executive authority. The duration of such closures may range from an early closure with normal operations expected on the next business day to a period of indeterminate length.

(c) At the time that a closure is declared, appropriate information, notifications, and instructions will be provided regarding the return to normal operations. The Contractor shall comply with all directives issued in regards to such closures. The Contractor shall follow agency procedures for registering emergency contact information and shall monitor appropriate broadcast mediums for receiving emergency information.

(d) When a closure is declared, contractor personnel must vacate the facility as directed except personnel designated in accordance with agency procedures by the contracting officer to remain onsite to continue performance. Evacuated personnel will not be allowed to reenter the facility for the duration of the closure. Performance of work at alternate sites is not permissible except in accordance with the terms of the contract and written authorization by the contracting officer.

(e) Whenever it is necessary for contractor employees to continue performance during such closures, the contracting officer will provide written authorization for such work. Such written authorization will designate the specific individuals authorized to continue performance, alternate work sites when applicable, work schedules, work dates, and special instructions and information. Telework may be authorized if permitted by the terms of the contract. Any services scheduled to be performed at Government facilities shall not be performed elsewhere unless specifically authorized in accordance with the terms of this contract.

(f) For firm fixed priced contracts, the terms for invoicing and payment in the contract will remain unchanged unless changed by a fully executed modification to the contract.

(g) For other than firm fixed priced contracts, the contractor shall invoice in accordance with the Payments and Prompt Payment clauses of the contract only for work performed. Employee compensation for the period of the closure shall be governed by corporate policy.

(h) Agency-sponsored events such as picnics or other social events are not considered to be official office closures. The Contractor shall not invoice for time spent by its employees attending or participating in such events.

(i) In no case will any compensable administrative leave, which might be approved for Federal employees in connection with official holidays or other events, extend to contractor personnel.

[End of clause]

☐ **DEA-2852.219-70 SECTION 8(a) DIRECT AWARD (MAY 2012)**

(a) Pursuant to the Partnership Agreement (PA) between the U.S. Small Business Administration (SBA) and the U.S. Department of Justice (DOJ), the U.S. Drug Enforcement Administration (DEA), a component of the DOJ, hereby executes a direct award to **[enter name of 8(a) concern]** under the authority delegated to it by the SBA in accordance with 13 CFR 124.501 and the PA. DEA will perform all contract execution and review functions pertaining to this award in accordance with the delegation. The DEA will notify the SBA of this award, as required by 13 CFR 124.503(a)(4)(ii), and provide SBA with a copy of the award.

(b) Notwithstanding the identification of the parties on the award form, the prime Contractor for this award is the U.S. Small Business Administration, and **[enter name of 8(a) concern]** is the Subcontractor.

(c) The cognizant SBA district office is:

[SBA district office]

[street address]

[city, state and zip code]

(d) **[enter name of the 8(a) concern]** shall:

(1) Notify the Contracting Officer, simultaneous with its notification to the SBA (as required by SBA's 8(a) regulations at 13 CFR 124.308), when the owner or owners upon whom 8(a) eligibility is based plan to relinquish ownership or control of the concern. Consistent with Section 407 of Public Law 100-656, transfer of ownership or control shall result in termination of the contract for convenience, unless the SBA waives the requirement for termination prior to the actual relinquishing of ownership and control;

(2) Comply with the applicable performance requirements of clause 52.219-14, Limitations on Subcontracting as checked below: [*Contracting officer: check only one performance standard based on the primary purpose of the contract.*]

☐ *Services (except construction)* — At least 50 percent of the cost of contract performance incurred for personnel shall be expended for employees of the concern.

☐ *Supplies (other than procurement from a nonmanufacturer of such supplies)* — The concern shall perform work for at least 50 percent of the cost of manufacturing the supplies, not including the cost of materials.

☐ *General construction* — The concern will perform at least 15 percent of the cost of the contract, not including the cost of materials, with its own employees.

☐ *Construction by special trade contractors* — The concern will perform at least 25 percent of the cost of the contract, not including the cost of materials, with its own employees.

(3) Provide the contracting officer with evidence of compliance with the applicable performance standard. This report shall show total dollars expended in the cost category specified in the performance standard both for the reporting period and cumulative to date along with the dollars and percentage of total dollars expended from the contractor's resources. This report shall be submitted annually. A final report covering the entire period of the contract shall be submitted upon expiration of the contract.

(4) Not subcontract the performance of any of the requirements of this contract without the prior written approval of the Contracting Officer.

(e) Compliance with the Limitation on Subcontracting clause is a mandatory performance requirement of this contract.

(End of clause)

☒ **DEA-2852.222-70 APPLICABLE WAGE DETERMINATION (SERVICE CONTRACT LABOR STANDARDS) (APR 2021)**

(a) In accordance with clause 52.222-41, Service Contract Labor Standards, the minimum monetary wages and fringe benefits applicable to this contract are set forth in the attached Wage Determination(s):

Wage Determination #	Revision #	Date	Section J Attachment #
2015-5231	**32**	**May 13, 2026**	

(b) The Contractor shall attach a copy of this (these) wage determination(s) to Wage and Hour Division (WHD) poster WH-1313, Employee Rights on Government Contracts, and shall post both the publication and the wage determination(s) in a prominent and accessible location in the workplace as required by Federal Acquisition Regulation 22.1018(c). WH-1313 is available for downloading at http://www.dol.gov/whd/regs/compliance/posters/sca.htm (*Spanish language version available at http://www.dol.gov/whd/regs/compliance/pdf/scaspan.pdf*).

(c) The Contractor shall classify each service employee who will perform under this contract by the applicable wage determination according to the work performed by the employee. If the applicable wage determination does not include an appropriate occupational code, title, and wage rate for a service employee employed under the contract, the Contractor shall initiate the conformance process in accordance with paragraph (c) of clause 52.222-41 and corresponding instructions provided by the WHD at https://www.dol.gov/sites/dolgov/files/WHD/legacy/files/SCA_Conformance_Guide.pdf.

(End of clause)

☐ **DEA-2852.231-70 TRAVEL REQUIREMENTS FOR CONTRACTORS (APR 2023)**

Contractor personnel may be required to conduct travel in the performance of this contract. All travel must be pre-approved in writing by the Contracting Officer's Representative (COR) or the Task Monitor (TM). Any expenses incurred by Contractor personnel without prior Government approval will be denied for payment. The Contractor will be reimbursed for travel costs in accordance with Part 31 of Federal Acquisition Regulation (FAR) and the Federal Travel Regulation (FTR).

Travel requirements shall use the most cost effective and efficient means of transportation. All travel should be scheduled in advance in order to take advantage of discounted rates. The Contractor shall engage only the minimum number of travelers and vehicles needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible. Commuting expenses between an employee's residence and duty station are not reimbursable and will be disallowed.

DOMESTIC TRAVEL

Contractors are authorized to use commercial air, commercial rail, rental vehicle, Government vehicle as a passenger, company authorized vehicle, or privately owned vehicle when travel is approved. When a mode other than commercial air is contemplated, the Contractor shall contact the COR to determine the mode of travel most advantageous to the Government. Domestic U.S. travel rates (i.e., per diem, mileage, etc.) can be found on the General Services Administration (GSA) website under the Travel Resources section.

DEA encourages travelers to use shuttles, either complimentary/courtesy or for a fee, as the first preference for ground transportation. When considering a rental car, once the authorizing official determines that a rental car is necessary and cost effective, ensure that the rental is covered by government rental car contract.

The Contractor may be authorized for usual taxicab and airport taxicab fares, when applicable, plus tips, from a common carrier or other terminal to either the employee's home or place of business, from the employee's home or place of business to common carrier terminal, or between airport and airport limousine terminal.

When suitable common carrier transportation is available but the traveler elects to use a taxicab, an explanation of the circumstances should be furnished on the travel voucher and reimbursement will be at the travel voucher approving official's discretion. Taxicab reimbursement in excess of $75.00 plus tip (not to exceed 20% of the fare,) must be supported by a receipt. The election of any expensive mode of transportation, including luxury services, are not allowable.

Reimbursement may also be authorized or approved for the usual taxicab fares, plus tip, as follows:

a) From the employee's home to office on the day of departure from the office on an official trip requiring at least one night's lodging; and
b) From office to home on the day of return to the office from such a trip.
c) To obtain meals at the nearest available place when they cannot be obtained at the TDY station or place of lodging. Travelers must remark on their travel voucher that there was no restaurant at their place of lodging or within walking distance of the lodging or TDY location.

If authorized lodging, the traveler should book hotel reservations through a Travel Management Center (TMC) at the same time they book their airfare.

If lodging is not found within the maximum lodging rate, a request for actual lodging costs must be authorized in advance by the SES-level SAC, Regional Director, HQ

Office Head, Administrator or Deputy Administrator. This authority may not be redelegated.

OVERSEAS NON-FOREIGN AREAS/INTERNATIONAL TRAVEL

Maximum rates of per diem allowances and reimbursements for miscellaneous travel expenses for travel in Alaska, Hawaii, Guam, Puerto Rico and territories and possessions of the United States are prescribed by the Department of Travel Management Office (DTMO) located on DTMO's website at (http://www.defensetravel.dod.mil/site/perdiem.cfm).

The Contractor shall be responsible for ensuring that all employees scheduled to travel to international locations have a valid passport. DEA will not request or authorize the issuance of a "US Official Government" passport for contractor personnel.

International travel to specific countries and regions may be subject to additional DoS requirements, as well as host nation requirements, such as visas. The Contractor shall be responsible for complying with any applicable DoS and destination national requirements and notifying the COR/ TM of any matters that impact cost, schedule, or performance.

Maximum rates of per diem allowance and reimbursements for miscellaneous travel expenses for travel in foreign areas, including the Trust Territory of the Pacific Islands, are established by the DoS (https://aoprals.state.gov/web920/per_diem.asp).

LIMITATION OF GOVERNMENT LIABILITY FOR CONTRACTS PERFORMED OUTSIDE OF THE UNITED STATES

This contract requires performance in whole or in part by contractor employees in one or more locations outside of the United States. By entering into the contract, the contractor assumes certain risks associated with performance including risks of injury to or death of its employees. The Contractor shall be responsible for notification of the employee-designated next of kin in the event of injury or death. The contractor may elect to obtain and maintain private insurance to cover those risks or cover the risks with its own resources. Any mandatory requirement for insurance will be specified in the contract in an appropriate insurance clause as prescribed in FAR subpart 28.3. The Government assumes no liability for any costs associated with performance of the contract not expressly stipulated in the contract.

In no event will the Government indemnify the contractor for any third-party liability.

TRAVEL INVOICE

Travel expenses shall not include fees calculated as profit. General and Administrative (G&A) expenses shall be allowable on travel costs, provided that the Contractor's accounting system has been accepted by the Defense Contract Auditing Agency (DCAA). DEA reserves the right to negotiate a ceiling on all travel costs. Travel costs incurred by subcontractors may not be subsequently "marked up" by a prime Contractor's G&A prior to submission to DEA.

The Contractor must submit a travel invoice upon the completion of travel. The travel invoice must be submitted to the COR in accordance with the invoice clause or the timetable specified in the subject contract. The invoice must contain all required documentation, including receipts supporting the travel costs and evidence of DEA pre-authorization to travel. The documentation shall include the following information: traveler's name(s), purpose of travel, destination, Contract Number, Task Order Number (if applicable), Contract Line Item Number (CLIN), name of DEA official authorizing the travel, date of authorization and a breakdown of actual travel costs. If applicable, the travel cost breakdown for per diem shall include: total number of travel days, lodging, miscellaneous and incidental expenses (including tolls, mileage, etc.), differential and allowances, with subtotals by category and a grand total. Vouchers and receipts shall be attached to invoices.

(End of clause)

☐ **DEA-2852.237-70 PREVENTING PERSONAL SERVICES CONTRACTS AND PERFORMANCE OF INHERENTLY GOVERNMENT FUNCTIONS (JUN 2018)**

(a) A personal services contract is characterized by the employer-employee relationship it creates between the Government and the contractor's personnel. This contract action is for non-personal services and is not a personal services contract action. Due to the need for close interaction of government and contractor personnel, it is essential for all contractor personnel for this contract performing at Drug Enforcement Administration (DEA) designated worksites to receive supervision from their parent company and avoid employer-employee relationships with government officials. In addition, it is important for contractor personnel to recognize and avoid circumstances that may appear to be personal services. Federal Acquisition Regulation (FAR) subpart 37.104 provides important information to be aware of to avoid performing these types of duties. The contractor awarded this contract shall ensure their employees and subcontractors comply with this requirement and receive supervision from their parent company to avoid performance of a personal services contract.

(b) "Inherently governmental function" means, as a matter of policy, a function so intimately related to the public interest as to mandate performance by Government employees. An inherently governmental function includes activities requiring either the exercise of discretion in applying Government authority, or the making of value judgments in making decisions for the Government. Governmental functions normally fall into two categories: the act of governing, *i.e.,* the discretionary exercise of Government authority, and monetary transactions and entitlements. It is essential for all contractor personnel performing services at DEA designated worksites to recognize and understand what inherently government functions are. Federal Acquisition Regulation (FAR) subpart 7.5 - Inherently Governmental Functions and the Office of Management and Budget's (OMB) Office of Federal Procurement Policy (OFPP) Policy Letter 11-01, Performance of Inherently Governmental and Critical Functions, provide important information regarding inherently governmental functions to be aware of to avoid performing these types of duties. The contractor awarded this contract shall ensure their employees and subcontractors comply with this requirement.

(c) Contractors providing personnel who perform services on-site at DEA offices must certify via the "Contractor Employee Certification Concerning Prohibition of Personal Services Contracts and Inherently Governmental Functions" form that its on-site employee(s) have read and understand FAR 37.104, Personal services contracts, and FAR subpart 7.5 before they may begin work at an on-site DEA office. The Contractor on-site supervisor shall address any questions or concerns with the Contracting Officer's Representative (COR) or Contracting Officer.

(End of Clause)

☐ **DEA-2852.239-71 INFORMATION RESELLERS OR DATA BROKERS (MAY2012)**

(a) Under this contract, the Drug Enforcement Administration (DEA) obtains personally identifiable information about individuals from the contractor.

(b) The Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonable believed to have been, breached. Any notification shall be coordinated with the DEA, and shall not proceed until the DEA has made a determination that notification would not impede a law enforcement investigation or jeopardize national security.

(c) The method and content of any notification by the contractor shall be coordinated with, and be subject to the approval of, the DEA/DOJ. The Contractor assumes full responsibility for taking corrective action consistent with the DEA's Guidelines for Data Breach Notification (December 2, 2011), which may include offering credit monitoring when appropriate.

(End of clause)

☐ **DEA-2852.239-74 CERTIFICATION OF OPERABILITY ON SYSTEMS USING THE FEDERAL DESKTOP CORE CONFIGURATION OR THE UNITED STATES GOVERNMENT CONFIGURATION BASELINE (MAY 2012)**

(a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC) or the United States Government Configuration Baseline (USGCB). This includes Internet Explorer 7 and 8 configured to operate on Windows XP, Windows Vista, and Windows 7 (in Protected Mode on Windows Vista and Windows 7).

- For the Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html.
- For the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html.
- For Windows 7 settings, see: http://usgcb.nist.gov/usgcb_content.html.

(b) The standard installation, operation, maintenance, updating, and/or patching of software shall not alter the configuration settings from the approved FDCC or USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.

(c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

(End of clause)

☒ **DEA-2852.242-70 CONTRACTOR PERFORMANCE ASSESSMENT (MAR 2020)**

(a) Pursuant to FAR subpart 42.1502(e), the Government will assess the Contractor's performance under this contract. Performance assessment information may be used by the Government for decision-making on exercise of options, source selection, and other purposes, and will be made available to other federal agencies for similar purposes.

(b) Performance will be assessed in the following areas:

(1) Quality of product or service;
(2) Schedule;
(3) Cost control;
(4) Business relations;
(5) Management of key personnel; and
(6) Other appropriate areas.

(c) For contracts that include the clause at 52.219-9, Small Business Subcontracting Plan, performance assessments will consider performance against, and efforts to achieve, small business subcontracting goals set forth in the small business subcontracting plan.

(d) For any contract with a performance period exceeding 18 months, inclusive of all options, the Government will perform interim performance assessments annually and a final performance assessment upon completion of the contract.

(e) The Government will prepare contractor performance assessment reports electronically using the Contractor Performance Assessment Reporting System (CPARS). Additional information on CPARS may be found at www.cpars.gov.

(f) The Contractor will be provided access to CPARS to review performance assessments. The Contractor shall designate a CPARS point-of-contact for each contract subject to performance assessment reporting. Upon setup of a contract in CPARS, the Contractor's CPARS point-of-contact will receive a system-generated e-mail with information and instructions for using CPARS. Prior to finalizing any contractor performance assessment, the Contractor shall be given 14 calendar days to review the report and submit comments, rebutting statements, or additional information. Disagreements between the Contractor and the Government performance assessment official will be resolved by a Government Reviewing Official, whose decision on the matter will be final.

(g) The Government will also report in the Federal Awardee Performance and Integrity Information System (FAPIIS) module of CPARS information related to:

(1) A Contracting Officer's final determination that a contractor has submitted defective cost or pricing data;

(2) Any subsequent change to a final determination concerning defective cost or pricing data pursuant to 15.407-1(d);

(3) Any issuance of a final termination for default or cause notice; or

(4) Any subsequent withdrawal or a conversion of a termination for default to a termination for convenience.

(End of clause)

☒ **DEA-2852.242-71 INVOICE REQUIREMENTS (DEC 2022)**

(a) In order to initiate processing for payment, the Contractor shall submit scanned or electronic images of invoice(s) to the following e-mail address: *[enter*

Process Coordinator title, organization, and invoicing e-mail address]. The Contractor shall also send an informational copy of the invoice to the following addressee(s):

(1) [enter contract specialist's or purchasing agent's name & e-mail address]; and

(2) Contracting Officer's Representative: [enter COR's name & e-mail address or else enter N/A if COR has not been appointed].

(b) The date of record for invoice receipt is established on the day of receipt of the e-mail if it arrives before the end of standard business hours (5 p.m. local), or the next business day if the invoice arrives outside of normal business hours. Scanned documents with original signatures in .pdf or other graphic formats attached to the e-mail are acceptable. Digital/electronic signatures and certificates cannot be processed by DEA and will be returned.

(c) In addition to the items required in FAR 32.905(b), a proper invoice shall also include the following minimum additional information and/or attached documentation:

(1) Total/cumulative charges for the billing period for each Contract Line Item Number (CLIN);

(2) Dates upon which items/services were delivered; and

(3) The Contractor's Taxpayer Identification Number (TIN).

(d) Invoices will be rejected if they are illegible or otherwise unreadable, or if they do not contain the required information or signatures.

(End of Clause)

☒ **DEA-2852.242-72 FINAL INVOICE AND RELEASE OF RESIDUAL FUNDS (MAY 2012)**

(a) The Contractor shall submit a copy of the final invoice to the Contracting Officer at the address listed in clause DEA-2852.242-71, Invoice Requirements. The final invoice must be marked "Informational Copy – Final Invoice."

(b) By submission of the final invoice and upon receipt of final payment, the Contractor releases the Government from any and all claims arising under, or by virtue of, this contract. Accordingly, the Government shall not be liable for the payment of any future invoices that may be submitted under the above referenced order.

(c) If residual funds on the contract total $100 or less after payment of the final invoice, the Government will automatically deobligate the residual funds without further communication with the vendor.

(d) If funds greater than $100 remain on this order after payment of the final invoice, the Government will issue a bilateral modification to deobligate the residual funds. The contractor will have up to **TBD** calendar days after issuance of the modification to sign and return it. The contractor's signature on the modification shall constitute a release of all claims against the Government arising by virtue of this contract, other than claims, in stated amounts, that the Contractor has specifically exempted from the operation of the release. If the contractor fails to sign the modification or assert a claim within the stated period, the Government will deobligate the residual balance and proceed with close-out of the contract.

(End of clause)

☒ **DEA-2852.242-74 CONTRACT ADMINISTRATION POINTS OF CONTACT (MAY 2012)**

(a) The Contract Administration Office for this contract is:

U. S. Department of Justice
Drug Enforcement Administration
Office of Acquisition (FA)
8701 Morrissette Drive
Springfield, VA 22152

Contract Specialist/telephone #/email:

Contracting Officer/telephone #/email: TBD

Contracting Officer's Representative (COR): See DEA-2852.242-73

(b) Contract administration for the contractor shall be performed by:

Name: (enter name, title, mailing address, telephone #, and e-mail address)

(End of clause)

☒ **DEA-2852.242-81 CONTRACTOR RECORDS MANAGEMENT REQUIREMENTS (SEP 2020)**

A. Applicability

This clause applies to all contractors whose employees create, receive, or maintain federal records as defined below in Section B.

B. Definitions

"Federal record," 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a federal agency under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. DEA Federal Records include records created, received, or maintained by the contractor its employees, agents, or subcontractors pursuant to this contract; and, deliverables and documentation associated with deliverables. Personal materials are not considered federal records.

C. Requirements

1. The contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, and 33), NARA regulations at 36 C.F.R. Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. § 552a). These policies include the preservation of all DEA records, regardless of form or characteristics, mode of transmission, or state of completion.
2. In accordance with 36 C.F.R. § 1222.32, all data created for government use and delivered to, or falling under the legal control of the government are federal records subject to the provisions of 44 U.S.C. Chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. § 552), as amended, and the Privacy Act of 1974 (5 U.S.C. § 552a), as amended, and must be managed and scheduled for disposition only as permitted by statute or regulation.
3. In accordance with 36 C.F.R. § 1222.32, the contractor shall maintain all DEA records created for DEA use or created in the course of performing this contract and/or delivered to, or under the legal control of the government, and records must be managed in accordance with federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.
4. DEA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records shall not be destroyed except in accordance with the provisions of the agency records schedules and with concurrence of the DEA Contracting Officer. Records may not be removed from the legal custody of DEA without the written concurrence of the Deputy Assistant Administrator, Office of Acquisition and Relocation Management. Willful and unlawful destruction, damage, or alienation of federal records is subject to the fines and penalties imposed by 18 U.S.C. § 2701. In the event that the contractor determines that there has been an unlawful or accidental unauthorized destruction, accidental removal, or alteration of federal records within its control, or within the control of its employees and agents, the contractor shall immediately report the incident to the DEA Contracting Officer of all facts and circumstances related to the discovered destruction or removal. The DEA Contracting Officer must advise DEA's Office of Administration, Freedom of Information and Records Management Section (FSR) of any such incidents and FSR must report promptly to NARA in accordance with 36 C.F.R. § 1230.
5. The contractor shall immediately notify the appropriate DEA Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records, or equipment. Disclosure of non-public information is limited to authorized personnel with a need to know as described in this contract. The contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of DEA information, data, documentary material, records, and/or equipment are properly protected. The contractor shall not remove material from DEA facilities or systems, or facilities or systems operated or maintained on the DEA's behalf, without the express written permission of the Deputy Assistant Administrator, Office of Acquisition and Relocation Management. When information, data, documentary material, records, and/or equipment is no longer required, it shall be returned to DEA's control or the contractor must hold it until otherwise directed. Items returned to DEA shall be hand carried, mailed, emailed, or securely electronically transmitted to the DEA Contracting Officer or address prescribed in this contract. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).
6. The contractor is required to obtain the DEA Contracting Officer's approval prior to engaging in any contractual relationship (sub-contract) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The contractor (and any subcontractor) is required to abide by government and DEA guidance for protecting sensitive, proprietary, classified, and controlled unclassified information. The contractor shall:
    - Incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under DEA awarded contracts, and require written subcontractor acknowledgment of same.
    - Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor
7. The contractor shall only use government-furnished equipment or resources for purposes specifically tied to or authorized by the contract.
8. The contractor shall not create or maintain any records containing any non-public DEA information that are not specifically tied to or authorized by the contract.
9. Notwithstanding the Rights in Data clause of the contract, the contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that is exempt from disclosure by the Freedom of Information Act.
10. In accordance with the Rights in Data clause of the contract, DEA reserves its rights to data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which DEA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.
11. Training. All contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take DEA provided records management training. The contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

D. Flowdown of requirements to subcontractors

1. The contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract/order, and require written subcontractor acknowledgement of the requirements.
2. Violation by any subcontractor of any provision set forth in this clause will be attributed to the contractor.

(End of clause)

☐ **DEA-2852.242-82 DOJ REPORTING SYSTEM FOR REPORTABLE PERSONNEL SECURITY RELATED ACTIVITIES (APR 2023)**

This clause is applicable if the contract or order includes clause DOJ-03, *Personnel Security Requirements for Contractor Employees and Alternate I—Classified Information—Cleared Contractors*. The Department of Justice (DOJ) *iReport* system is a secure, web-based application used by personnel to report activities as required by section 6 – *Employee Reporting Requirements* of clause DOJ-03. Use of the *iReport* system is mandatory for contractor employees having access to it through Firebird. Employees who do not have access to *iReport* must submit reports directly to the cognizant Contracting Officer's Representative and to the DEA Security Program Manager by email to ISR.Correspondence@dea.gov. Additional guidance and instruction on the use of the *iReport* system may be viewed at https://dojnet.doj.gov/jmd/seps/persg/ireport.php.

(End of clause)

☐ **DEA-2852.242-80 TELECOMMUTING AND REMOTE WORK ARRANGEMENTS FOR CONTRACTOR EMPLOYEES (AUG 2023)**

(a) Notwithstanding the terms of the contract that require performance at the Government's site, the Government may authorize the Contractor to perform work under this contract at locations other than the place(s) of performance specified elsewhere in the contract; provided, that the contract does not expressly prohibit telecommuting in the performance of the contract and that telecommuting or remote work would not jeopardize the requirements of the contract, including security requirements. The term "telecommuting" applies to contractor employees within the local commuting area where the Government site is located and who may be authorized to work at locations other than the Government's site. The term "remote work" applies to contractor employees within the local commuting area where the Government site is located

(b) The COR, in conjunction with the cognizant Program Office must make a written determination that:

(1) Certain work functions or the missions of certain work units are suitable for a telecommuting or remote work arrangement;

(2) The Contractor is suitable for a telecommuting or remote work arrangement based on individual performance, program requirements and mission objectives;

(3) Summary of work performed during telecommuting hours is submitted to the COR on a bimonthly basis;

(4) The Contractor shall sign and submit the completed Contractor Telecommuting and Remote Work Agreement Form;

(5) The COR shall retain the signed Contractor Telecommuting and Remote Work Agreement Form in the contract file for record keeping and provide a copy to the Contracting Officer;

(6) The Contractor shall obtain the necessary technology prior to teleworking:

(i) Firebird Anywhere - http://intranet/sites/si/Mobile/fba/Pages/default.aspx; OR

(ii) DEA issued Laptop--If the contractor's current computer is a desktop, the Program Office may request a laptop using a DEA-19 form for the Contractor to take home when teleworking.

(7) The COR and the Contractor shall review and re-sign, if approved, the Contractor Telecommuting and Remote Work Agreement on an annual basis. - Contractor Telecommuting and Remote Work Agreement

(8) The COR or the Contractor reserve the right to terminate the Contractor Telecommuting and Remote Work Agreement at any time.

(c) Under no circumstance will the Contractor be authorized to perform any work requiring access to DOJ/DEA information or information systems unless such access will be made exclusively using DEA equipment or property issued for this purpose.

(d) No authorization for alternate work locations shall be construed as an indication of past performance, an increase in the price of the contract, an approval of overtime, a change in the contract schedule, or approval of an accelerated rate of expenditures.

(e) Local commuting expenses incurred in traveling to or from any approved alternate work location are not reimbursable. Any incidental costs incurred in performing work at approved alternate work locations will be reimbursable in accordance with the Allowable Cost and Payment clause and the Payments clause of the contract, provided that such costs are segregated and allocable to the contract.

(f) The Contractor is responsible for protecting and using any DEA-owned or provided equipment or other property for official purposes only. DEA is

responsible for servicing, and maintaining any DEA-provided equipment issued to the Contractor. DEA is not liable for injuries or damages to the Contractor's personal or real property while the Contractor is working at the approved telework location.

(End of clause)

☒ **DEA-2852.247-70 GENERAL PACKAGING AND MARKING REQUIREMENTS (MAY 2012)**

(a) Packaging and packing for all items (includes written materials, reports, presentations, etc.) delivered hereunder shall be in accordance with common commercial practices, adequate to insure protection from possible damage resulting from improper handling, inclement weather, water damage, excessive heat and cold, and to insure acceptance by a common carrier for safe delivery to its final destination.

(b) All deliverables shall clearly indicate the contract number and/or task (delivery) order number, as appropriate, on or adjacent to the exterior shipping label.

(End of clause)

☒ **DOJ-01 WHISTLEBLOWER INFORMATION DISTRIBUTION (OCT 2021)**

Within 30 days of contract award, the contractor and its subcontractors must distribute the "Whistleblower Information for Employees of DOJ Contractors, Subcontractors, Grantees, or Sub-Grantees or Personal Services Contractors" ("Whistleblower Information") document to their employees performing work in support of the products and services delivered under this contract (https://oig.justice.gov/sites/default/files/2020-04/NDAA-brochure.pdf). By agreeing to the terms and conditions of this contract, the prime contractor acknowledges receipt of this requirement, in accordance with 41 U.S.C. § 4712 and FAR 3.908 & 52.203-17, and commits to distribution. Within 45 days of award, the contractor must provide confirmation to the contracting officer verifying that it has distributed the whistleblower information as required. version includes all of the information in the English language document.

(End of clause)

☒ **DOJ-02 CONTRACTOR PRIVACY REQUIREMENTS (JAN 2022)**

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) *Privacy Act Information*

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984) and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires Contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DOJ system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.justice.gov/opcl/doj-systems-records.[1] Applicable SORNs published by other agencies may be accessed through those agencies' websites or by searching the Federal Digital System (FDsys) available at http://www.gpo.gov/fdsys/. SORNs may be updated at any time.

(2) *Prohibition on Performing Work Outside a Government Facility/Network/Equipment*

Except where use of Contractor networks, IT, other equipment, or Workplace as a Service (WaaS) is specifically authorized within this contract, the Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or WaaS and Government information shall remain within the confines of authorized Government networks at all times. Any handling of Government information on Contractor networks or IT must be approved by the Senior Component Official for Privacy of the component entering into this contract. Except where remote work is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of remote work authorizations.

(3) *Prior Approval Required to Hire Subcontractors*

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(4) *Separation Checklist for Contractor Employees*

The Contractor shall complete and submit an appropriate separation checklist to the Contracting Officer before any employee or Subcontractor employee terminates working on the contract. The Contractor must submit the separation checklist on or before the last day of employment or work on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposition of personally identifiable information (PII)[2], in paper or

[1] "[T]he term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4). "[T]he term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).

[2] As stated in FAR 52.224-3 and Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource (2016), "'personally

electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to PII or other sensitive information.

In the event of adverse job actions resulting in the dismissal of a Contractor or Subcontractor employee before the separation checklist can be completed, the Prime Contractor must notify the Contracting Officer within 24 hours and confirm receipt of the notification. In the case the Contractor is unable to notify the Contracting Officer, then the Contractor should notify the Contract Officer's Representative (COR).

Contractors must complete the separation checklist with the Contracting Officer or COR by returning all Government-furnished property including, but not limited to, computer equipment, media, credentials and passports, smart cards, mobile devices, Personal Identity Verification (PIV) cards, calling cards, and keys and terminating access to all user accounts and systems. Unless the Contracting Officer requests otherwise, the relevant Program Manager or other Key Personnel designated by the Contracting Officer or COR may facilitate the return of equipment.

B. Privacy Training, Safeguarding, and Remediation

(1) *Required Security and Privacy Training for Contractors*

The Contractor must ensure that all employees take appropriate privacy training, including Subcontractors who have access to PII as well as the creation, use, dissemination and/or destruction of PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle PII, including heightened security requirements for the transporting or transmission of sensitive PII, and reporting requirements for a suspected breach or loss of PII. These courses, along with more information about DOJ security and training requirements for Contractors, are available at https://www.justice.gov/jmd/learndoj. The Federal Information Security Modernization Act of 2014 (FISMA) requires all individuals accessing DOJ information to complete training on records management, cybersecurity awareness, and information system privacy awareness. Contractor employees are required to sign the "Privacy Rules of Behavior," acknowledging and agreeing to abide by privacy law, policy, and certain privacy safeguards, prior to accessing DOJ information. These Rules of Behavior are made available to all new users of DOJ's computer network and to trainees at the conclusion of DOJ-OPCL-CS-0005.

The Contractor should maintain copies of certificates as a record of compliance and must submit an email notification annually to the COR verifying that all employees working under this contract have completed the required privacy and cybersecurity training.

(2) *Safeguarding PII Requirements*

Contractor employees must comply with DOJ Order 0904 and other guidance published to the publicly-available Office of Privacy and Civil Liberties (OPCL) Resources page[3] relating to the safeguarding of PII, including the use of additional controls to safeguard sensitive PII (e.g., the encryption of sensitive PII). This requirement flows down from the Prime Contractor to all Subcontractors and lower tiered subcontracts.

(3) *Non-Disclosure Agreement Requirement*

Prior to commencing work, all Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (NDA) and the DOJ IT Rules of Behavior. The Non-Disclosure Agreement:

(a) prohibits the Contractor from retaining or divulging any PII or other sensitive information, or derivatives therefrom, furnished by the Government or to which they may otherwise come in contact as a result of their performance of work under the contract/task order that is otherwise not publicly available, whether or not such information has been reduced to writing; and

(b) requires the Contractor to report any loss of control, compromise, unauthorized disclosure, or unauthorized acquisition of PII or other sensitive information to the component-level or headquarters Security Operations Center within one (1) hour of discovery.

The Contractor should maintain signed copies of the NDA for all employees as a record of compliance. The Contractor should also provide copies of each employee's signed NDA to the Contracting Officer before the employee may commence work under the contract/task order.

(4) *Prohibition on Use of PII in Vendor Billing and Administrative Records*

The Contractor's invoicing, billing, and other financial or administrative records or databases is not authorized to regularly store or include any sensitive PII or other confidential government information that is created, obtained, or provided during the performance of the contract without the written permission of the Senior Component Official for Privacy (SCOP). It is acceptable to list the names, titles and contact information for the Contracting Officer, COR, or other personnel associated with the administration of the contract in the invoices as needed.

(5) *Reporting Actual or Suspected Data Breach*

Contractors must report any actual or suspected breach of PII within one hour of discovery.[4] A "breach" is an incident or occurrence that involves the loss of control,

identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Regarding "sensitive PII," "[t]he sensitivity level of the PII will depend on the context, including the purpose for which the PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed. For example, the sensitivity level of a list of individuals' names may depend on the source of the information, the other information associated with the list, the intended use of the information, the ways in which the information will be processed and shared, and the ability to access the information." OMB Circular A-130, at App. II-2.

[3] The DOJ OPCL Resources page is available at https://www.justice.gov/opcl/resources.

[4] As stated in DOJ Instruction 0900, "Contractors must notify the Contracting Officer, the Contracting Officer's Representative, and JSOC (or component-level SOC)

compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. The report of a breach must be made to DOJ. The Contractor must cooperate with DOJ's inquiry into the incident and efforts to minimize risks to DOJ or individuals, including remediating any harm to potential victims.

(a) The Contractor must develop and maintain an internal process by which its employees and Subcontractors are trained to identify and report the breach, consistent with DOJ Instruction 0900.00.01[5], Reporting and Response Procedures for a Breach of Personally Identifiable Information.

(b) The Contractor must report any such breach by its employees or Subcontractors to the DOJ Security Operations Center (dojcert@usdoj.gov, 202-357-7000); Component-level Security Operations Center and Component-level Management Team, where appropriate; the COR; and the Contracting Officer within one (1) hour of the initial discovery.

(c) The Contractor must provide a written report to the DOJ Security Operations Center (dojcert@usdoj.gov, 202-357-7000) within 24 hours of discovery of the breach by its employees or Subcontractors. The report must contain the following information:

(i) Narrative or detailed description of the events surrounding the suspected loss or compromise of information.[6] Date, time, and location of the incident.
(ii) Amount, type, and sensitivity of information that may have been lost or compromised, accessed without authorization, etc.
(iii) Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.[7]
(iv) Names and classification of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
(v) Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.[8]
(vi) Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
(vii) Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

(d) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(e) At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access PII or to work on that contract based on their actions related to the loss or compromise of PII.

(6) *Victim Remediation*

At DOJ's request, the Contractor is responsible for notifying victims and providing victim remediation services in the event of a breach of PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose PII was lost or compromised. When DOJ requests notification, the Department Chief Privacy and Civil Liberties Officer and SCOP will direct the Contractor on the method and content of such notification to be sent to individuals whose PII was breached. By performing this work, the Contractor agrees to full cooperation in the event of a breach. The Contractor should be self-insured to the extent necessary to handle any reasonably foreseeable breach, with another source of income, to fully cover the costs of breach response, including but not limited to victim remediation.

C. Government Records Training, Ownership, and Management

(1) *Records Management Training and Compliance*

The Contractor must ensure that all employees and Subcontractors that have access to PII as well as to those involved in the creation, use, dissemination and/or destruction of PII take the *DOJ Records and Information Training for New Employees (RIM)* training course or another training approved by the Contracting Officer or COR. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and
every year thereafter.
The Contractor shall maintain copies of certificates as a record of compliance and must submit an email notification annually to the COR verifying that all employees working under this contract have completed the required records management training.

(a) The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of

within 1 hour of discovering any incidents, including breaches, consistent with this Instruction, guidance issued by the CPCLO, NIST standards and guidelines, and the US-CERT notification guidelines."

[5] https://www.justice.gov/file/4336/download

[6] As stated in DOJ Instruction 0900, the description should include the type of information that constitutes PII; purpose for which PII is collected, maintained, and used; extent to which PII identifies a peculiarly vulnerable population; the determination of whether the information was properly encrypted or rendered partially or completely inaccessible by other means; format of PII (e.g., whether PII was structured or unstructured); length of time PII was exposed; any evidence confirming that PII is being misused or that it was never accessed.

[7] As stated in DOJ Instruction 0900, the report should include the nature of the cyber threat (*e.g.*, Advanced Persistent Threat, Zero Day Threat, data exfiltration) for cyber incidents.

[8] As stated in DOJ Instruction 0900, the report should include analysis on whether the data is accessible, usable, and intentionally targeted.

records containing PII and those covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

(2) *Records Creation, Ownership, and Disposition*

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency information. The Contractor shall certify, in writing, the appropriate disposition or return of all Government information at the conclusion of the contract or at a time otherwise specified in the contract. In accordance with 36 CFR 1222.32, the Contractor shall maintain and manage all Federal records created in the course of performing the contract in accordance with Federal law. Records may not be removed from the legal custody of DOJ or destroyed except in accordance with the provisions of the agency records schedules.

(b) Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and may be considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. § 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.

D. Data Privacy and Oversight

1. *Restrictions on Testing or Training Using Real Data Containing PII*

The use of real data containing PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible.

2. *Requirements for Contractor IT Systems Hosting Government Data*

The Contractor is required to obtain an Authority To Operate (ATO) for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

3. *Requirement to Support Privacy Compliance*

(a) If this contract requires the development, maintenance or administration of information technology[9], the Contractor shall support the completion of the Initial Privacy Assessment (IPA) document, if requested by Department personnel. An IPA is the first step in a process to identify potential privacy issues and mitigate privacy risks. The IPA asks basic questions to help components assess whether additional privacy protections may be needed in designing or implementing a project[10] to mitigate privacy risks, and whether compliance work may be needed. Upon review of the IPA, the OPCL determines whether a Privacy Impact Assessment (PIA) document and/or SORN, or modifications thereto, are required. The Contractor shall provide adequate support to complete the applicable risk assessment and PIA document in a timely manner, and shall ensure that project management plans and schedules include the IPA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DOJ, including IPAs, PIAs, and SORNs, is located on the DOJ OPCL website (https://dojnet.doj.gov/privacy/), including DOJ Order 0601, Privacy and Civil Liberties. The Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy risk assessment and documentation, the Contractor shall provide adequate support to DOJ to ensure DOJ can complete any required assessment, and IPA, PIA, SORN, or other supporting documentation to support privacy compliance. The Contractor shall work with personnel from the program office, OPCL, the Office of the Chief Information Officer (OCIO), and the Office of Records Management and Policy to ensure that the privacy assessments and documentation are kept on schedule, that the answers to questions in the documents are thorough and complete, and that questions asked by the OPCL and other offices are answered in a timely fashion. The Contractor must ensure the completion of required PIAs and documentation of privacy controls consistent with federal law and standards, e.g. NIST 800-53, Rev. 5; and compliance with the Privacy Act of 1974, E-Government Act of 2002, Federal Information Security Modernization Act of 2014, and key OMB guidelines, e.g., OMB

[9] As defined in 40 U.S.C. § 11101, the term "information technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract.

[10] In this instance, the term "project" is used to scope the activities (e.g., creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, or disposing of information) covered by an IPA. A project is intended to be technology-neutral, and may include an information system, a digital service, an information technology, a combination thereof, or some other activity that may create potential privacy issues or privacy risks that would benefit from an IPA. The scope of a project covered by an IPA is discretionary, but components should work with their SCOP and OPCL.

Circular A-130.

(End of Clause

☐ **DOJ-03 PERSONNEL SECURITY REQUIREMENTS FOR CONTRACTOR EMPLOYEES (NOV 2021) and ALTERNATE I—CLASSIFIED INFORMATION—CLEARED CONTRACTORS (NOV 2021)**

Work performed under this contract will involve any one or more of the following: access to DOJ Information, which may include Controlled Unclassified Information (CUI), i.e., unclassified, sensitive DOJ information, and/or access to DOJ Information Technology (IT) systems, and/or unescorted access to DOJ space or facilities. Contractor employees will occupy Public Trust Positions, unless clause alternates are applied.

☐ ***(Check if applicable) Access to/safeguarding of classified information will be required. ALTERNATE I sections also apply.***

1. GENERAL REQUIREMENTS

(a) (1) All references to "contract(or) personnel" and "contract(or) employee" in this clause means all individuals, without limitation, to include individuals employed by the contractor, team member, subcontractor, consultant, and/or independent contractor, who will have access to information of the Department of Justice (DOJ) or information that is within the custody and control of the DOJ, access to DOJ IT systems, and/or unescorted access to DOJ facilities/space in connection with the performance of this contract. "Employment" as used herein does not create nor imply an employer/employee relationship between the DOJ and contractor employees.

(ALTERNATE I) [The following is added to the clause]: (2) Additionally, work performed under this contract will involve access to classified information [National Security Information (NSI)].

(b) (1) The type of security investigation required for each contractor employee will be governed by the type and risk level of information made available to the contractor employee. The contractor will not be permitted to commence performance under this contract until a sufficient number of its personnel, as determined by the Security Programs Manager (SPM), in consultation with the Contracting Officer's Representative if one is appointed, have received the requisite security approval.

(ALTERNATE I) [The following is added to the Clause]: (2) All contractor employees requiring access to classified information will be processed by Defense Counterintelligence and Security Agency (DCSA) in accordance with the National Industrial Security Program (NISP). The contractor will not be permitted to commence performance under this contract until a sufficient number of its personnel, as determined by the SPM in consultation with the Contracting Officer's Representative (COR) if one is appointed, have received the requisite NSI Clearance.

(c) Except where specifically noted otherwise, the federal government will be responsible for the cost and conduct of the investigation.

(d) The contractor shall ensure that no contractor employee commences performance prior to receipt of a written authorization from the contracting officer, COR, or the SPM that performance by the respective contractor employee is authorized.

(e) The data and other information to which the contractor may have access as a result of this contract is the property of, and/or within the custody and control of, the Department, and its disclosure to third parties is governed by various statutes and regulations, the violation of which may subject the discloser to criminal penalties.

2. CITIZENSHIP AND RESIDENCY REQUIREMENTS

(a) *Residency Requirement*. (1) Contractor employees in Public Trust positions, both U.S. citizens and non-U.S. citizens, must meet the Department's residency requirement if they will require access to DOJ information, IT systems, or unescorted access to facilities. For three years (not necessarily consecutive years) out of the last five years immediately prior to employment under the Department contract the contractor employee musthave: (i) resided in the U.S.; (ii) worked for the U.S. in a foreign country as either an employee or contractor in a federal civilian or military capacity; or, (iii) been a dependent of a federal civilian or military employee or contractor working for the U.S. in a foreign country. At the Department's sole discretion, the residency requirement may be waived by the Department Security Officer (DSO) for contractor employees on a case-by-case basis where justified by extenuating circumstances. The residency requirement does not apply to contractor employees residing in foreign countries that are hired to work in American embassies/consulates/missions located outside of the United States and who require access to DOJ information, IT systems, or unescorted access *provided that* an adequate background investigation can be conducted, with favorable adjudication, as determined by the DSO.

(ALTERNATE I) ***[The following is added to the clause]:*** **(2) The residency requirement does not apply to contractor employees working on the classified portion of this contract whose national security clearance has been processed by DCSA in accordance with the NISP.**

(b) *Citizenship*. (1) Aside from the specific exceptions set forth in Section 1.2(b)(2), for Public Trust positions, the DOJ requires that contractor employees be U.S. citizens and nationals, or lawful permanent residents seeking U.S. citizenship. Any prospective non-U.S. citizen contractor employee who requires access to DOJ information systems, DOJ information, and/or unescorted facilities access must also have been granted a waiver as described below in paragraphs 1.2(d) and/or (e). The contractor is responsible for verifying that the non-U.S. citizens working under this contract are lawful permanent residents seeking U.S. citizenship.

(2) *Exception for Certain Non-U.S. Citizen Contractor Employees*: (i) Non-U.S. citizen expert witnesses, litigative consultants, and interpreters in rare foreign languages are not required to be lawful permanent residents seeking U.S. citizenship. However, they must be granted a waiver for access to unclassified DOJ information, whether CUI or not, DOJ IT systems, and/or unescorted facility access, as described below in paragraph 1.2(d) and (e), regardless of the duration of their duties. (ii) Non-U.S. Citizen contractor employees residing in foreign countries who are hired to work for the Department of Justice in American embassies/consulates/missions outside of the United States are not required to be lawful permanent residents seeking U.S. citizenship.

(ALTERNATE I) *[The following is added to the clause]: (3) Contractor employees requiring access to classified information will be processed by DCSA in accordance with the NISP.*

(c) *Dual Citizenship*. (1) U.S. citizens who hold dual citizenship with a foreign country are considered U.S. citizens within the meaning of this clause, and may be considered for, but are not entitled to, contract employment as U.S. citizens consistent with this clause. The means by which the contractor employee obtained or exercises his or her dual citizenship status will be a consideration in the Public Trust Investigation (PTI) adjudication, and/or waiver approval processes discussed in this clause.

(ALTERNATE I) ***[The following is added to the clause]: (2) Contractor employees requiring access to classified information will be processed by DCSA in accordance with the NISP.***

(d) *Access to DOJ Information Technology Systems*. Non-U.S. citizens are not authorized to access DOJ information technology (IT) systems or assist in the development, operation, management, or maintenance of DOJ IT systems, including providing IT system support, unless a waiver has been granted by the Head of the DOJ component or designee, with the prior concurrence of both the DSO and the DOJ Chief Information Officer, allowing computer access by the non-U.S. citizen. Such a waiver will be granted only in exceptional and unique circumstances on a case-by-case basis. It should be noted that the Justice Consolidated Office Network (JCON) is a sensitive DOJ IT system and any contractor employee who will need access to JCON must be a U.S. citizen or have received a waiver. In order for a waiver to be considered for approval: (1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; (2) The type of personnel security vetting that has been conducted on the individual, and vetting results, that would mitigate risk; and (3) The waiver must be in the best interest of the federal government.

(e) *Access to Unclassified DOJ Information and Unescorted Access to DOJ Facilities or Space*. (1) Except as provided under 1.2(b)(2), non-U.S. citizens are not authorized to access DOJ information and/or unescorted access to DOJ facilities or space, unless a waiver has been granted by the DSO, allowing access by the non-U.S. citizen. Such a waiver will be granted on a case-by-case basis where justified at the discretion of the DSO.

3. BACKGROUND INVESTIGATION REQUIREMENTS

(a) (1) Unless otherwise stated below, all contractor personnel are subject to a Public Trust Investigation (PTI). The SPM will determine the type of investigation for each contractor employee based on the risk category (i.e., the nature of the position and degree of harm that could be caused by the individual in that position) and whether the position is long-term or short-term. The PTI risk categories are listed below.

(i) High Risk Positions. The minimum background investigation required is a Tier 4 (T4) investigation, and the five-year reinvestigation required is a Tier 4R (T4R) investigation. The 2017 version of the Standard Form (SF) 85P, Questionnaire for Public Trust Positions, is required.

(ii) Moderate Risk Positions. The minimum background investigation required is a Tier 2 (T2) investigation. The five-year reinvestigation required is a Tier 2R (T2R) investigation. The 2017 version of the SF-85P is required.

(iii) Low Risk/Non-Sensitive Positions. The minimum background investigation required for Low Risk/Non-Sensitive positions is a Tier 1 (T1) investigation and the required five-year reinvestigation is also a Tier 1 (T1) investigation. The SF 85, Questionnaire for Non-Sensitive Positions, is required.

(ALTERNATE I) ***[The following is added to the clause]:*** *(2). Contractor employees requiring access to classified information will be processed by DCSA in accordance with the NISP.*

(b) *Exception for Expert Witnesses*. Expert Witnesses, litigative consultants, and interpreters in rare foreign languages may not be subject to full background investigation requirements if alternative security requirements are approved by the DSO.

(c) *Short-Term U.S. Citizen Contractor Employees*. Other than the exception in Section 1.3(b), short-term contractor employees (6 months or less) who are U.S. citizens are not subject to a full background investigation, however, must receive an approved pre-employment background investigation waiver. The required forms to complete and submit are listed in Section 1.4(b) and (c)(2).

(d) *Long-Term U.S. Citizen Contractor Employees*. Other than the exception in Section 1.3(b), all long-term U.S. citizen employees (longer than 6 months) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(e) *Non-U.S. Citizen Contractor Employees*. Other than the exception in 1.3(b), all non-U.S. citizen contractor employees regardless of performance duration (short or long term) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(f) *Reciprocity*. (1) A Public Trust Investigation will be accepted under reciprocity if it meets the following guidelines: (i) the investigation is current (investigations are considered current if completed within the last five years) and favorably adjudicated, or the reinvestigation has been deferred; (ii) the investigation meets or exceeds the level of investigation required for the DOJ contractual instrument; (iii) there has been no continuous (not cumulative) break in federal contract/service employment of two years or more; (iv) there is no derogatory information since the favorable fitness determination or adjudication that calls into question the individual's fitness based on character or conduct; and (v) the investigative record does not show conduct that is incompatible with the core duties of the new contract position. A "core duty" is a continuing responsibility that is of particular importance to the relevant covered position or the achievement of an agency's mission. Core duties will vary from position to position.

(ALTERNATE I) ***[The following is added to the clause]*****: (g) National security investigations will be accepted from other federal agencies under reciprocity guidelines provided all of the following are true: (i) The new position does not require a higher eligibility than what the subject currently possesses; (ii) the existing eligibility is not granted on an interim or temporary basis, or limited or one-time basis; (iii) the covered individual's eligibility is not currently denied, revoked, or suspended; (iv) the favorable adjudication was based on the 13 Adjudicative Guidelines (SEAD 4) and E.O. 12968. Agencies may accept eligibility recorded with an exception based on their own risk assessment; (v) the most recent background investigation is not more than seven years old; (vi) there is no new derogatory information of national security adjudicative relevance that has been reported/developed since last investigation; (vii) the Bond Amendment disqualifier (SEAD 4) does not apply and individual requires SCI, SAP, or restricted access; and (viii) the subject does not have a break in federal service of 24 months or longer.**

4. BACKGROUND INVESTIGATION PROCESS

(a) *e-QIP (or its successor)*. Public Trust background investigations/reinvestigations of contractor employees will be performed by the DCSA. The investigative process requires contractor employees to complete the Electronic Questionnaires for Investigations Processing (e-QIP) and provide additional information as specified in paragraph 1.4(b) below. Immediately after contract award, the contractor shall designate an employee as its "e-QIP Initiator" and provide the name of this person to the SPM. The e-QIP Initiator must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being given access to e-QIP. After the e-QIP Initiator's security approval is granted, the Contractor will be configured in e-QIP as a sub-agency to DOJ. The contractor will then be responsible for initiating investigations for all contract personnel, whose previous investigation does not meet reciprocity, in e-QIP for completion of the security questionnaire form and forwarding the electronic form with the remainder of the security package to the SPM. Subject to the prior written approval of the SPM, the contractor may designate an e-QIP Initiator for each subcontractor. Subcontractor e-QIP Initiators must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being provided access to e-QIP.

(b) *Additional Documentation*. (1) In addition to completing the e-QIP questionnaire (see 1.4(a), above), the contractor shall ensure that each contractor employee occupying Public Trust Positions, including short-term employees, completes and submits the following information through the contractor's Corporate Security Officer:

(i) Digital Fingerprinting/FD-258 Applicant Fingerprint Card. Two sets are required per applicant. The contractor may schedule appointments with the SPM to be digitally fingerprinted; otherwise, fingerprinting by the FBI or other law enforcement entity, as approved by the SPM, is required to ensure the identity of the person being fingerprinted and for printing quality. All pertinent information must be completed by the individual taking the fingerprints (FBI or other). Use of the physical FD-258 Applicant Fingerprint Card should only be used in extenuating circumstances.

(ii) DOJ-555 Fair Credit Reporting Act Disclosure. Authorizes DOJ to obtain one or more consumer/credit reports on the individual. This form will be required if the Component SPM determines a credit check is necessary for its Low Risk Level 1 contractor positions.

(iii) OF-306, Declaration for Federal Employment.

(iv) Foreign National Relatives or Associates Statement. This is only required if foreign national relatives or associates were not disclosed on the security questionnaire form.

(v) Self-Reporting Requirements for All Contractor Personnel. This is an acknowledgement and acceptance statement that every contractor must sign.

(vi) Additional information as may be required based on the review of the security questionnaire form.

The contractor shall review all forms/documents to ensure each is complete, accurate and meets all DOJ requirements, including applicable residency and citizenship requirements. The contractor shall resolve any issues or discrepancies with the contractor employee, including resubmission of corrected forms or documentation. Completed forms/documents shall be submitted to the SPM (or designee, which may include the COR) within five (5) calendar days after being finalized.

(c) *Adjudication and Pre-Employment Background Investigation Waivers*

(1) Except as set forth in this section, background investigations must be conducted and favorably adjudicated for each contractor employee prior to commencing their work on this contract. Where programmatic needs do not permit the federal government to wait for completion of the entire background investigation, a pre-employment background investigation waiver for *public trust contractors* can be granted by the SPM, in consultation with the cognizant COR. Pre-employment waivers cannot be used to circumvent delays in clearing classified contractors through the DCSA, if access to classified information is required.

(2) As directed by the SPM, the contractor shall initiate pre-employment waivers for Public Trust Positions when necessary. This may entail performing credit history checks and submission of these checks as part of the security package, including satisfactory resolution of any issues prior to submission to the federal government. A waiver will be disapproved if it develops derogatory information that cannot be resolved in the contractor employee's favor. When a waiver has been disapproved, the CO, in consultation with the SPM and COR, will determine (i) whether the contractor employee will no longer be considered for work on a DOJ contract or (ii) whether to wait for the completion and favorable adjudication of the background investigation before the contractor employee commences work on a Department contract. The pre-employment background investigation waiver requirements include:

1. Verification of citizenship (copy of a birth certificate, naturalization certificate, or U.S. passport);
2. Verification of compliance with the *DOJ Residency Requirement* of this Clause;
3. Favorable review of the security questionnaire form;
4. Favorable FBI fingerprint results;
5. Favorable credit report;
6. Favorable review of the OF-306 form, Declaration for Federal Employment;
7. Verification of the initiation of the appropriate background investigation (for long-term personnel); and
8. Receipt of the signed DOJ *Self-Reporting Requirements for All Contractor Personnel* (see Section 1.6, below).

(3) The investigating agency (DCSA) will provide the SPM with the results of each proposed contractor employee's Public Trust investigation. Upon receipt of the investigation and any other pertinent documents from the investigating agency, the SPM will determine whether each proposed contractor employee should be granted employment security approval.

(4) The COR will notify the contractor of the results of Public Trust background investigations as they are completed and adjudicated, including any individual who is found ineligible for employment security approval. For any individual found ineligible for employment on a Department contract, the contractor shall propose a replacement and initiate the background investigation process consistent with this clause.

(ALTERNATE I) ***[The following is added to the clause]:***

(5) (1) For classified contracts, the contractor shall possess or be capable of obtaining a Department of Defense Central Adjudication Facility (DODCAF) Defense Industrial Security Clearance Facility Cage Code and the security clearance required to fully perform this contract. As directed by the COR or SPM, the contractor shall submit the information necessary to allow the Government to prepare and obtain for the Contractor a "Department of Defense Contract Security Classification Specification" (DD Form 254) for this contract. Where such clearance is required, the contractor agrees to provide information and access to contractor facilities as may be required by federal government investigators.

(2) Immediately after contract award (or post-award receipt of the required Facility Clearance), the contractor's Facility Security Officer (FSO) shall furnish to the COR a list of all personnel proposed to work under this contract who have been processed in accordance with the NISP by the DCSA. The contractor shall update this information as individuals are added or separated from the contract and the FSO shall provide the updated list to the COR.

(3) For each contractor employee who requires access to classified information under this contract, the contractor shall forward a Visit Authorization Request (VAR) indicating the current background investigation information and clearance level to the COR.

5. IDENTITY PROOFING AND BADGING

(a) Access to DOJ Information, federally-controlled IT systems, and/or unescorted access to federally-controlled facilities or space (regardless of whether the contractor employee will be issued a DOJ PIV card or building access badge) shall be made available after each respective contractor employee has (1) met the identity proofing requirements outlined below, and (2) completed all other security requirements stated elsewhere in this contract.

(b) (1) Public Trust contractor employees must appear in person at least once before a DOJ official or an official of a trusted contract company (i.e., has a facility security clearance) who is responsible for checking two forms of identification in original form prior to commencement of work by the contractor employee

and PIV card or building access badge issuance (as applicable). Approval will be documented by the DOJ official or an official of a trusted contract company. (Acceptable documents are listed in Form I 9, Employment Eligibility Verification, and at least one document must be a valid state or federal government issued picture ID).

(c) (ALTERNATE I) ***[The following is added to the clause]:*** **(2) All contractor employees requiring access to classified information must appear in person at least once before an official of the contractor possessing the facility clearance, who is responsible for checking the identification documents. (Acceptable documents are listed in Form I 9, Employment Eligibility Verification, and at least one document must be a valid state or federal government issued picture ID). This identity proofing must be completed prior to commencement of work by the contractor employee under this contract and badge issuance (as applicable) and must be documented by the contractor official.**

(d) All contractor employees requiring unescorted access to a DOJ controlled facility or space shall comply with the PIV card or building access badge requirements outlined below:

(i) When any contractor employee enters a DOJ building for the first time, he/she shall allow one hour for security processing and the creation and issuance of a building access badge. PIV cards require additional processing time and will not likely be issued on the same day.

(ii) Building access badges shall be subject to periodic review by the contractor employee's supervisor and checked against his/her personal identification. The contractor employees shall present themselves for the issuance of renewed badges when required by the government as scheduled by the COR or his/her designee. The contractor shall notify the COR when contractor employee badges are lost, and must immediately apply for reissuance of a replacement badge. The contractor shall pay for reissued building access badges at no cost to the government. It is the contractor employee's responsibility to return badges to the COR or his/her designee when a contractor employee is dismissed, terminated or assigned to duties not within the scope of this contract.

6. EMPLOYEE REPORTING REQUIREMENTS

All contractor employees must sign the DOJ *Self-Reporting Requirements for All Contractor Personnel* statement acknowledging and accepting the DOJ requirement that they immediately self-report certain information using the Department's iReport system. The COR or SPM will provide the Self-Reporting statement as well as a list of reportable information, which varies by position sensitivity designation, to the contractor employee before commencing work under the contract. If the contractor employee does not have access to the DOJ iReport System, the COR or SPM will provide a fillable form for the contractor employee to complete and submit.

(a) The COR and SPM will review the written report and documentation and make a determination regarding continued employment on a DOJ contract.

(b) DOJ reporting requirements are in addition to the DCSA reporting requirements and the contractor's internal reporting requirements.

7. REPLACEMENT PERSONNEL

(a) The contractor shall make every effort to avoid costs to the government for security investigations for replacement of contractor employees, and in so doing shall ensure that otherwise satisfactorily performing and physically able contractor employees remain in contract performance for the duration of the contract. The contractor shall take all necessary steps to ensure that contractor personnel who are selected for assignment to thiscontract are professionally qualified and personally reliable, of reputable background and sound character, and able to meet all other requirements stipulated in the contract.

(b) The fact that the government performs security investigations shall not in any manner relieve the contractor of its responsibility to ensure that all contract personnel are reliable and of reputable background and sound character. Should a security investigation conducted by the government and/or a contractor's self-report or failure to self-report render ineligible a contractor employee, the contracting officer will determine whether the contractor has violated this clause. The contracting officer may direct the contractor, at its own expense, to remove and replace any contractor personnel who fails to comply with or violates applicable requirements of this contract. Such action may be taken at the government's direction without prejudice to its rights under any other provision of this contract, including termination for default, and the contractor may be held liable, at a minimum, for all reasonable and necessary costs incurred by the government to (i) provide coverage (performance) through assignment of individuals employed by the government or third parties in those cases where absence of contractor personnel would cause either a security threat or DOJ program disruption and (ii) conduct security investigations in excess of those which would otherwise be required.

(c) Nothing in this clause shall require the contractor to bear costs involved in the conduct of security investigations for replacement of a contractor employee who separates from the contractor of his/her own accord, is incapacitated, or is deceased.

(d) The contractor shall comply with the terms and conditions set forth under this clause and assumes all liability for failure to comply. The rights and remedies conferred upon the government by this clause are in addition to all and other rights and remedies pursuant to the contract and as established by law.

(End of Clause)

☐ **Security of Department Information and Systems DOJ-05 (APR 2026)**

I. Applicability to Contractors and Subcontractors

Section 2839.102 of the Justice Acquisition Regulation (JAR), (48 C.F.R. § 2839.102), applies to this contract. Accordingly, all contractors are obligated to comply with all applicable DOJ security policies, directives, or guidance documents, including the security requirements in the provisions in this contract clause. This contract clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of the contractors and subcontractors (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. The security requirements set forth herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), and any other applicable laws, mandates, contract clauses, DOJ policies, directives or guidance documents and Executive Orders pertaining to the development and operation of Information Systems and/or the protection of Government Information. This clause does not alter or diminish any existing rights, obligations, or liability under any other civil and/or criminal law, rule, regulation, or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. **Authorization to Operate** ("ATO"), as defined in National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-37 Revision 2, is the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls.

B. **Cloud Computing**, as defined in DOJ Order 0904 Cybersecurity Program, 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models in accordance with NIST SP 800-145.

C. **Covered Contract** is any contract, order or other agreement under which the contractor, or a subcontractor at any tier, including a cloud service provider, may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information (as defined below) in the course of providing a product or service to the Department, with the exception of acquisitions under the micro-purchase threshold.

D. **Covered Information System** means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information under a Covered Contract.

E. **Data** means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data, computer software, and personally identifiable information (PII) (defined below). The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

F. **DOJ Information**, as defined in DOJ Order 0904, means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by the Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired to perform the contract.

G. **Information,** as defined in DOJ Order 0904, is any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. This includes any communication or representation of knowledge in an electronic format that allows it to be stored, retrieved, or transmitted.

H. **Information System**, means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)).

I. **Personally Identifiable Information ("PII")**, as defined in the FAR 24.101, means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. It includes but is not limited to common data elements such as names, addresses, dates of birth, and places of employment, to identity documents, Social Security numbers or other government-issued identifiers, precise location information, medical history, and biometric records. This definition covers all PII that is created by or becomes available to the contractor, including its employees, subcontractors, or affiliates, as a result of performing under this contract. PII, as supplementally defined in DOJ Order 0904, also includes information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity.

J. **Private Cloud**, as defined in NIST SP 800-145, is the deployment model for cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

K. **Security Breach** means any security incident (as defined below) that directly relates to the loss of control, compromise, exfiltration, manipulation, unauthorized disclosure, unauthorized acquisition, unauthorized exposure or unauthorized access or any similar occurrence of any Covered Information System or any DOJ Information or any PII accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system. This includes incidents where (1) a person other than an authorized user accesses or potentially accesses PII or DOJ Information or (2) an authorized user accesses or potentially accesses PII or DOJ Information for an unauthorized purpose.

a. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed security breach (as defined above).
b. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed security breach (as defined above).

L. **Security Incident** means any occurrence that (1) may actually or imminently jeopardize, without lawful authority, the availability, integrity, authentication, confidentiality, or nonrepudiation of DOJ Information or a Covered Information System; or (2) may constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

a. **Potential Security Incident** means any suspected, but unconfirmed security incident (as defined above).
b. **Confirmed Security Incident** means any confirmed security incident (as defined above).

M. **Vulnerability,** as defined in DOJ Vulnerability Management Plan, and the OCIO Information Security Management Procedure, means a weakness or flaw discovered in the design of a system that, when exploited, may result in a loss of confidentially, integrity, or availability of DOJ Information or an Information System.

III. Confidentiality and Non-Disclosure of DOJ Information

A. Preliminary and final contract deliverables and all associated working papers and material generated by the Contractor developed using DOJ Information, product, source code, and/or methods of operations, are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO")

or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14 (Rights in Data-General). The Contractor will define a method of monitoring the development activity to include any activity associated with DOJ Information, product, source code, and methods of operations. The data rights and development details shall be defined within the Contract.

If the Contractor intends to utilize its existing data, for which it has a patent or copyright, to develop a contract deliverable, it is incumbent upon the Contractor to negotiate with the CO the proper FAR Part 27 clauses in the contract to protect its existing data.

B. Pursuant to FAR 52.227-14(d)(2), all documents and data produced in the performance of this contract containing DOJ Information, product code, source code, and/or methods of operations are the property of the U.S. Government and, without the prior written permission of the CO, the Contractor shall neither reproduce nor release such information to any third-party at any time, including during performance or following expiration and/or termination of the contract.

C. Any DOJ Information made available to the Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, the Contractor assumes responsibility for the protection of the confidentiality of all DOJ Information processed, stored, or transmitted by the Contractor. The Contractor shall comply with information security responsibilities and duties throughout the contract and after expiration/termination as appropriate per contract close-out activities. When requested by the CO (typically no more than annually), the Contractor shall provide a report to the CO identifying, to the best of the Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, in addition to any other applicable requirements, as set forth in Part I, the Contractor shall comply with the security requirements of the Federal Information Security Modernization Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards as amended, and OMB Memoranda relating to the security of information and/or Federal Information Systems.

B. In addition, for all Covered Information Systems, the Contractor shall comply with the following requirements, which are listed here only to highlight certain specific applicable requirements from one of the sources identified in the first paragraph of this Section. This is not an exhaustive list of all such requirements with which the Contractor is obligated to comply, and the omission of a requirement from this list should not be construed as negating the materiality of that requirement. These requirements and those in the authorities in the prior paragraph should be read together.

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise.
2. Providing security awareness training at least annually to all Contractor employees and contractors involved with the Covered Contract. Such training shall include, but not be limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems.
3. Creating, protecting, and retaining, in accordance with applicable requirements but in any event at least until the expiration of the contract, Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information.
4. Maintaining authorizations to operate any Covered Information System.
5. Performing continuous monitoring on all Covered Information Systems, to include but not be limited to, collecting, reviewing, and analyzing appropriate logs and timely investigating security alerts and potential security incidents.
6. Establishing and maintaining baseline configurations and current inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Covered Information Systems.
7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups.
8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods as defined by NIST 800-63-3, *Digital Identity Guidelines* or current revision.
9. Establishing and maintaining an operational incident handling capability for Covered Information Systems that includes adequate and timely development, logging, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and timely reporting incidents to appropriate officials and authorities within the Contractor's organization and the DOJ.
10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance.
11. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media, and DOJ assets under Contractor control; protecting them from environmental impacts, access, and equipment positioning requirements defined; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media.
12. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized personnel according to DOJ 03.
13. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards including personnel background checks.
14. Continuously assessing the risk to DOJ Information in Covered Information Systems, including scanning and remediating vulnerabilities, or implementing appropriate mitigation in accordance with DOJ policy, and ensuring the timely removal of assets no longer supported by the Contractor.

15. Continuously monitoring the application of security controls of Covered Information Systems, assessing the efficacy of such controls, and developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Covered Information Systems.
16. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Covered Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security.
17. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate and timely action in response.
18. Ensuring return of Government Furnished Equipment ("GFE") and/or PIV card assets within 10 business days of notification for end of use (contract end, staff change, etc.).
19. Complying with rights in data (FAR 52.227-14) as to the development, management, and protection of DOJ Information.
20. Reporting on risks or known issues impacting DOJ Services (staffing, hardware, process, changes, etc.) through the Contractor's CO or COR, DOJ Service Owner ("SO"), and Government Technical Manager ("GTM") including risk mitigation activities.
21. Reporting through the Contractor's CO or COR on any projected or planned changes in corporate ownership, covered information system design, and/or any technical changes that could impact the confidentiality, integrity or availability of DOJ Information, data, or systems. Changes to system design must be updated through the authorization process per NIST SP 800-37 Revision 2, Step 6 ('Continuous Monitoring") or current NIST revision.
22. When, as part of operating within the DOJ environment, the Contractor's covered information system is subject to review, audit, or assessment by third parties, facilitating DOJ access to information system resources, facilities, personnel, and documentation in a timely manner as required by the auditors. Should a third-party organization conduct a review of any Covered Information System, the Contractor must provide a copy of the report to DOJ, through the CO and COR.
23. To enhance software supply chain and transparency, upon request, the Contractor shall provide a current Software Bill of Materials (SBOM) for all software, software updates, modules, libraries, and container images delivered or operated in the performance of this contract, consistent with applicable federal policy such as the National Telecommunications and Information (NTIA)-established minimum elements for SBOM to the CO who will refer to the DOJ Cyber-Security Risk Management team (C-SCRM) [Authority: OMB M-26-05; EO 14028/NTIA minimum requirements].
24. Reporting on outages impacting DOJ Services through the Contractor's CO, COR, and DOJ Service Owner (SO) to include event and mitigation details.

C. The Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an ATO for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. (For Cloud Computing Systems, see Section V, below.)

D. The Contractor shall ensure compliance with DOJ-03 (Personnel Security Requirements for Contractor Employees) as to all Covered Information Systems.

E. When requested by the DOJ CO or COR as described below, the Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to the Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, the Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

F. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause or access a Covered Information System is prohibited unless the CO approves it in writing after the Contractor has provided a letter certifying compliance with the following requirements. For any requirements which include the use or storage of PII, the Senior Component Official for Privacy must also approve. Any additional requirements set forth for the use or storage of PII under DOJ-02, Contractor Privacy Requirements, are in addition to, not superseded by, the requirements set forth here.

1. Media must be encrypted using a NIST FIPS 140-2 approved product.
2. The Contractor must develop and implement a process to ensure that security and other applications software is kept up to date.
3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism.
4. The Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information should be treated by the Contractor as sensitive information unless specifically designated as non-sensitive by the DOJ.
5. A Rules of Behavior (ROB) form must be signed and acknowledged annually by users. These rules must address, at a minimum, authorized, and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the users that they have no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.
6. Cybersecurity Awareness Training (CSAT) shall be provided annually by Contractor for all users of Covered Information System. This training must be submitted to, and approved by, the CO or COR in advance of being provided to users. Users must complete and acknowledge having received CSAT each year. At a minimum, CSAT provided by contractors must include:
    a. Insider Threat Detection and Reporting – Importance of detecting, methodologies, indicators, and reporting
    b. Privacy Awareness – Privacy Act and PII
    c. General Cybersecurity – Information security, trends in advance persistent threats, social engineering/phishing, appropriate use, mobile devices, remote access, basic security best practices

G. Contractors shall not store DOJ information on Contractor-owned removable IT (e.g., media such as a thumb drive or external hard drive) unless expressly authorized in writing by the DOJ CO or COR in the performance of their contract.

H. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.

I. The Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.

J. The Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 10 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information shall be returned in a format and form acceptable to DOJ. The Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 10 business days of the removal and return of all DOJ Information.

K. DOJ, at its discretion, may suspend the Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that the Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident or Security Breach (see definitions above), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Any termination action taken because of the Contractor's suspected failure to comply with any security requirement will be conducted in accordance with the applicable termination clause governing the awarded contract. The Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to DOJ, and that upon request by the CO, the Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at the Contractor's expense. The Contractor must comply with FAR 52.227-14 (Rights in Data), FAR 52.245-1 (Government Property), DOJ 2400.3A Chapter 1 (component property procedures), and FAR 4.804-5(a)(6) (Procedures for closing out contract files).

V. Cloud Computing

A. The Contractor may not utilize the Cloud system of any Cloud Service Provider ("CSP") unless:

1. All of the following has occurred: (a) the Cloud system and CSP have been evaluated by a Third Party Assessing Organization ("3PAO") certified under FedRAMP; (b) the Cloud system received FedRAMP authorization; (c) the Contractor has provided the most current System Security Plan ("SSP") and Security Assessment Report ("SAR") to the DOJ CO for consideration, and provides any subsequent SSPs and SARs within 30 days of issuance; and, (d) the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under the Covered Contract has issued an ATO; or,
2. In cases where the CSP or its offering is not FedRAMP authorized, the COR approves utilization of the Cloud System after the CSP has worked with the authorizing official, the DOJ OCIO, and the FedRAMP Program Management Office to determine that the CSP is likely to seek and receive Agency/FedRAMP authorization within 1 year, or DOJ has authorized use as a Private Cloud or Contractor Owned, Contractor Operated system.

B. The Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored, or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

C. The Contractor must ensure that the CSP provides access and information to support and enable DOJ's cloud security posture management, to include the current inventory of security management configuration data for services and information to confirm the Contractor has been monitoring accounts for compliance with security requirements. The DOJ Justice Security Operations Center (JSOC) must be able to access logs and events to investigate potential security breaches and perform security posture assessments associated with the Security Audit Identity Credential Access Management (ICAM) policies.

D. The Contractor must ensure that the CSP provides evidence of annual recertification of privileged user access management.

E. A C-SCRM review is mandatory for specified acquisitions in accordance with established process in EO 14028 and NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, or superseding document. All vendor products and solutions to be used on DOJ national security systems, enterprise-wide systems, or new FIPS-199 High and Moderate systems for the purpose of accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of DOJ Information must be submitted to DOJ OCIO for a C-SCRM review prior to contract award or ATO signature. Changes in corporate ownership or structure shall be reported to the CO for referral to C-SCRM. The Contractor shall notify the CO of any confirmed Supply Chain compromise affecting the Contractor's products or services within 1 hour of discovery.

_____ The following C-SCRM requirements for acquisition of systems, hardware, or software which will be used in systems that are mission critical or process sensitive data apply to this award. **(CO check as appropriate in coordination with the Program Manager and/or System Owner)**

1. The Contractor shall develop and deliver a C-SCRM Plan. The C-SCRM Plan shall meet the format described in NIST SP 800-161, Appendix E. The C-SCRM plan shall address the following security controls from NIST SP 800-53 Rev 5: SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-10, and SR-11. Equivalent ISO 27000 series controls may be used if they are mapped to the NIST control(s).
2. The Contractor shall implement the required security controls as documented in the C-SCRM Plan. The requirements of the C-SCRM plan shall flow down to all subcontractors. Evidence of the certification and compliance is required.
3. For cloud platforms or managed services, upon request, the Contractor shall provide a current SBOM of the runtime production environment reflecting the software components and dependencies materially present in the service.
4. The Contractor shall provide evidence of compliance with the documented C-SCRM Plan. **(CO select which applies**)

_____ Self-assessment by a contractor security team
_____ External assessment by an independent auditor

VI. Information System Security Incident

A. Confirmed Security Incident. The Contractor shall immediately (and in no event later than 1 hour of discovery) report any Confirmed Security Incident to the DOJ CO and COR. If the Confirmed Security Incident occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, the Contractor must call JSOC at 1-202-357-7000 immediately (and in no event later than within 1 hour of discovery of the Confirmed Security Incident) and shall notify the CO and COR as soon as practicable.

B. Potential Security Incident.

1. If the Contractor suspects that DOJ information has been potentially disclosed or impacted, the Contractor shall promptly investigate to determine if a Security Incident has occurred. If the Contractor has not determined within 24 hours (i.e., 24 hours from detection of potential security incident and/or security breach) whether the Potential Security Incident was in fact a Security Incident, then it must immediately report the Potential Security Incident to the DOJ CO and the COR. If the time by which to report the Potential Security Incident occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, the Contractor must call or e-mail the JSOC Team at 1-202-357-7000 or JSOC@USDOJ.GOV and contact the DOJ CO and COR as soon as practicable. If the contract involves PII, the Contractor must comply with the notification requirements of DOJ-02 and Executive Order M-17-12 (Memorandum on Preparing for and Responding to a Breach of Personally Identifiable Information), Contractor Privacy Requirements, Section B.5, for an actual or suspected Security Incident.
2. The Contractor must limit sharing of Security Incident details to only those individuals involved in responding to the potential Security Incident. Any provisions of the Covered Contract regarding the citizenship or location of individuals working on the Covered Contract apply equally to individuals involved in responding to any potential Security Incidents. The Contractor may request assistance from the JSOC for advice, incident response, or FBI coordination. The Contractor must provide weekly updates to CO, COR and JSOC during the course of a Security Incident investigation.

C. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify:

1. Both the Covered Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII.
2. All steps and processes being undertaken by the Contractor to minimize, remedy, and/or investigate the Security Incident.
3. Any and all other information as required by the CISA Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and

The Contractor may request assistance from the JSOC Team for advice, incident response, or FBI coordination, and must provide weekly updates to CO, COR, and JSOC during the course of an Incident investigation.

D. Except as otherwise required by Federal, State and local laws, executive orders, rules and regulations, all determinations regarding whether and when to notify other individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials, the DOJ Core Management Team, or the COR at DOJ's discretion.

E. The Contractor must provide to DOJ full access to any facility and/or Covered Information System affected or potentially affected by any potential or confirmed Security Incident, including access by the DOJ OIG and federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

F. DOJ, at its sole discretion, may obtain, and the Contractor will permit, the assistance of other federal agencies and/or third-party contractors or firms to aid in response activities related to any potential or confirmed Security Incident. Additionally, DOJ, at its sole discretion, may require the Contractor to retain, at the Contractor's expense, a 3PAO acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Covered Information Systems.

G. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by the Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. The Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

VII. Pass-Through of Security Requirements to Subcontractors and CSPs

A. The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with the contract, including any CSP providing services for any other CSP under the contract, and the Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to the Contractor.

(End of Clause)

☐ **DOJ-08 CONTINUING CONTRACT PERFORMANCE DURING A PANDEMIC INFLUENZA OUTBREAK OR OTHER BIOMEDICAL EMERGENCY OR CATASTROPHE (OCT 2007)**

During a Pandemic or other emergency, we understand that our contractor workforce will experience the same high levels of absenteeism as our federal employees. Although the Excusable Delays and Termination for Default clauses used in government contracts list epidemics and quarantine restrictions among the reasons to excuse delays in contract performance, we expect our contractors to make a reasonable effort to keep performance at an acceptable level during emergency periods.

The types of actions a federal contractor should reasonably take to help ensure performance are:

- Encourage employees to get inoculations or follow other preventive measures as advised by the public health service.

- Contractors should cross-train workers as backup for all positions performing critical services. This is particularly important for work such as guard services where telework is not an option.
- Implement telework to the greatest extent possible in the workgroup so systems are in place to support successful remote work in an emergency.
- Communicate expectations to all employees regarding their roles and responsibilities in relation to remote work in the event of a pandemic health crisis or other emergency.
- Establish communication processes to notify employees of activation of this plan.
- Integrate pandemic health crisis response expectations into telework agreements.
- With the employee, assess requirements for working at home (supplies and equipment needed for an extended telework period). Security concerns should be considered in making equipment choices; agencies or contractors may wish to avoid use of employees' personal computers and provide them with PCs or laptops as appropriate.
- Determine how all employees who may telework will communicate with one another and with management to accomplish work.
- Practice telework regularly to ensure effectiveness.
- Make it clear that in emergency situations, employees must perform all duties assigned by management, even if they are outside usual or customary duties.
- Identify how time and attendance will be maintained.

It is the contractor's responsibility to advise the government contracting officer if they anticipate not being able to perform and to work with the Department to fill gaps as necessary. This means direct communication with the contracting officer or in his/her absence, another responsible person in the contracting office via telephone or email messages acknowledging the contractor's notification. The incumbent contractor is responsible for assisting the Department in estimating the adverse impacts of nonperformance and to work diligently with the Department to develop a strategy for maintaining the continuity of operations.

The Department does reserve the right in such emergency situations to use federal employees. employees of other agencies, contract support from other existing contractors, or to enter into new contracts for critical support services. Any new contracting efforts would be acquired following the guidance in the Office of federal Procurement Policy issuance "Emergency Acquisitions", May, 2007 and Subpart 18.2. Emergency Acquisition Flexibilities, of the federal Acquisition Regulations.

(End of clause)

☒ **JAR 2852.201-70 CONTRACTING OFFICER'S REPRESENTATIVE (COR) (NOV 2020)**

(a) [name] of [organization], [address], [telephone number], [email address], is hereby designated to act as Contracting Officer's Representative (COR) under [award number], for the period of (specify the performance period of the contract that the designation covers).

(b) Performance of work under this contract is subject to the technical direction of the COR identified above, or another representative designated in writing by the Contracting Officer. The term ''technical direction'' includes, without limitation, the following:

(i) Receiving all deliverables;

(ii) Inspecting and accepting the supplies or services provided in accordance with the terms and conditions of this contract;

(iii) Clarifying, directing, or redirecting the contract effort, including shifting work between work areas and locations, filling in details, or otherwise serving to accomplish the contractual statement of work to ensure the work is accomplished satisfactorily;

(iv) Evaluating performance of the Contractor; and

(v) Certifying all invoices/vouchers for acceptance of the supplies or services furnished for payment.

(c) The COR does not have the authority to issue direction that:

(i) Constitutes a change of assignment or work outside the contract specification/work statement/scope of work.

(ii) Constitutes a change as defined in the clause entitled ''Changes'' or other similar contract term.

(iii) Causes, in any manner, an increase or decrease in the contract price or the time required for contract performance;

(iv) Causes, in any manner, any change in a term, condition, or specification or the work statement/ scope of work of the contract;

(v) Causes, in any manner, any change or commitment that affects price, quality, quantity, delivery, or other term or condition of the contract or that, in any way, directs the contractor or its subcontractors to operate in conflict with the contract terms and conditions;

(vi) Interferes with the contractor's right to perform under the terms and conditions of the contract; (vii) Directs, supervises, or otherwise controls the actions of the Contractor's employees or a Subcontractor's employees.

(d) The Contractor shall proceed promptly with performance resulting from the technical direction of the COR. If, in the opinion of the Contractor, any direction by the COR or the designated representative falls outside the authority of (b) above and/or within the limitations of (c) above, the Contractor shall immediately notify the Contracting Officer.

(e) Failure of the Contractor and Contracting Officer to agree that technical direction is within the scope of the contract is a dispute that shall be subject to the ''Disputes'' clause and/or other similar contract term.

(f) COR authority is not re-delegable.

(End of clause)

☐ **JAR 2852.222-70 DOMESTIC VIOLENCE, SEXUAL ASSAULT, AND STALKING (DEC 2014)**

(a) It is DOJ policy to enhance workplace awareness of and safety for victims of domestic violence, sexual assault, and stalking. This policy is summarized in ''*DOJ Policy Statement1200.02, Federal Workforce Responses to Domestic Violence, Sexual Assault, and Stalking,*'' available in full for public viewing at: *http://www.justice.gov/sites/default/files/ovw/legacy/2013/12/19/federal-workplaceeresponses-to-domesticviolence-sexualassault-stalking.pdf*. Vendor agrees, upon contract award, to provide notice of this Policy Statement, including at a minimum the above-listed URL, to all Vendor employees and employees of subcontractors who will be assigned to work on DOJ premises.

(b) Upon contract award, DOJ will provide the Contractor with the name and contact information of the point of contact for victims of domestic violence, sexual assault, and stalking for the component or components where the Contractor will be performing. The Contractor agrees to inform its employees and employees of subcontractors, who will be assigned to work on DOJ premises, with the name and contact information of the point of contact for victims of domestic violence, sexual assault, and stalking.

(End of Clause)

☒ **JAR 2852.223–70 UNSAFE CONDITIONS DUE TO THE PRESENCE OF HAZARDOUS MATERIAL (NOV 2020)**

(a) ''Unsafe condition'' as used in this clause means the actual or potential exposure of Contractor or Government employees to a hazardous material.

(b) ''Hazardous Material'' as used in this clause includes any material defined as hazardous under the latest version of Federal Standard No. 313 (including revisions adopted during the term of the contract), any other potentially hazardous material requiring safety controls, or any other material or working condition designated as hazardous by the Contracting Officer's Representative (COR).

(c) The Occupational Safety and Health Administration (OSHA) is responsible for issuing and administering regulations that require Contractors to apprise its employees of all hazards to which they may be exposed in the course of their employment; proper conditions and precautions for safe use and exposure; and related symptoms and emergency treatment in the event of exposure.

(d) Prior to commencement of work, Contractors are required to inspect for and report to the Contracting Officer the presence of, or suspected presence of, any unsafe condition including asbestos or other hazardous materials or working conditions in areas in which they will be working.

(e) If during the performance of the work under this contract, the Contractor or any of its employees, or subcontractor employees, discovers the existence of an unsafe condition, the Contractor shall immediately notify the Contracting Officer, or designee (with written notice provided not later than three (3) working days thereafter), of the existence of an unsafe condition. Such notice shall include the Contractor's recommendations for the protection and the safety of Government, Contractor and subcontractor personnel and property that may be exposed to the unsafe condition.

(f) When the Government receives notice of an unsafe condition from the Contractor, the parties will agree on a course of action to mitigate the effects of that condition and, if necessary, the contract will be amended. Failure to agree on a course of action will constitute a dispute under the Disputes clause of this contract.

(g) Nothing contained in this clause shall relieve the Contractor or subcontractors from complying with applicable Federal, State, and local laws, codes, ordinances and regulations (including the obtaining of licenses and permits) in connection with hazardous material including but not limited to the use, disturbance, or disposal of such material.

(End of Clause)

CONTRACTING OFFICER: List the recommended security clause in the approved DD 254 in the space provided below by clause number, title, and date of clause.

CONTRACTOR: The full text of the clause may be found at https://www.dea.gov/security-clauses.

Exhibit Number

ACKNOWLEDGEMENT OF CONTRACTOR RESPONSIBILITIES

The Drug Enforcement Administration ("DEA") acquires supplies and/or services from government Contractors (hereinafter, "Contractor(s)") performing under a DEA contract, task order, purchase order, delivery order, blanketpurchase agreement ("BPA"), reimbursable agreement ("RA"), and/or other type of contractual agreement (hereinafter, "Contract(s)"). As necessary, the Contractor may hire employees, officers, consultants, or subcontractors to perform under the Contract (hereinafter, "Contractor Personnel"). Contractor Personnel who work under such contractor agreements with the DEA must maintain satisfactory standards of competence, appearance, integrity and ethical conduct and shall be responsible for reporting violations of the terms of this document as well as allegations of misconductto the Contractor's Program Manager and the DEA Contracting Officer's Representative ("COR").

I. CONTRACTOR GENERAL RESPONSIBILITIES

The Contractor shall inform all Contractor Personnel of their duties, obligations, and responsibilities under the Contract. The Contractor shall obtain and make available, upon request by the Contracting Officer, a signed copy certifying that all Contractor Personnel participating in the performance of the Contract have reviewed, understand, and will comply with all of the provisions contained in this document.

The Contractor shall report, in writing, any violation of the Contractor Responsibilities document to the DEA COR, who must forward the report to DEA's Office of Security Programs/Personnel Security Section (ISR) Correspondence mailbox (ISR.Correspondence@dea.gov) within five (5) calendar days after the Contractor's initial notification to DEA. ISR will then make a suitability determination on the referred individual.

In accordance with DEA Clause 2852.204-80 Contractor Responsibility Form Certification, the Contractor shall certify that its employees read and sign this Contractor Responsibility Form before onboarding, and thereafter, annually on the anniversary date of employment.

A. SECURITY REQUIREMENTS

1. Personnel Security Requirements

a. The Contractor shall immediately inform the COR in writing when a Contractor Personnel or applicant on a DEA Contract has transferred to another contract, resigned, been terminated, or any other type of action that constitutes a break in the Contractor-employee relationship. The CORshall subsequently inform the Office of Security Programs of the same information at ISR.Security.Packages@dea.gov.

b. A mandatory periodic reinvestigation will be conducted once every five (5) years if the previous background investigation was based on the SF-85P and SF-85PS, Questionnaires for Public TrustPositions. A mandatory periodic reinvestigation will be conducted once every five (5) years on all public trust positions. Contractors under the National Industrial Security Program will be reinvestigated in accordance with Defense Counterintelligence and Security Agency policy. The same suitability and security standards that are required for new applicants apply to reinvestigations.

c. The Contractor has a continuing obligation to notify the COR, in writing, of any change in marital status of Contractor Personnel. As soon as possible, the Contractor must provide the COR with thefollowing information:

i. Change in status: married, divorced, or widowed.

ii. Date, city, and country of marriage, divorce, or death of spouse.

iii. Full name of current or former spouse (if notifying of a marriage, include wife's maiden name and any former married name(s)).
iv. New spouse's social security number, date of birth, and place of birth (city, state, and country).
v. New spouse's citizenship (include as applicable: alien registration number, date and place of entry into the United States, date and place of naturalization including courthouse and complete address, and citizenship certificate number).

d. The COR shall subsequently inform the Office of Security Programs of the same information at ISR.Security.Packages@dea.gov.

e. If an applicant was assigned to a DEA contract for a period of at least one (1) year, but less than five (5) years and is being considered for placement on the same or another DEA contract, the Contractorshall submit the following forms to the COR to update the criminal record and credit report queries:
i. Contract Personnel's Authorization to Conduct Agency-Specific Record Checks;
ii. DOJ-555 Revised Oct. 2008, Disclosure and Authorization Pertaining to Consumer Reports,
Pursuant to the Fair Credit Reporting Act; and
iii. Release—Fair Credit Reporting Act Of 1970, as amended; and the information regarding change in marital status, if applicable. With satisfactory results of the updated record queries,the COR will request the ISR to reactivate the individual's access to DEA facilities and information.
iv. The same suitability and security standards that are required for new applicants apply to reinvestigations.

2. Information Security Requirements

Contractor shall notify all Contractor Personnel having access to DEA information that such information may be used only for the purpose and to the extent authorized in the Contract, and that disclosure of any information, by any means, for a purpose or to an extent unauthorized herein, maysubject the offender to criminal sanctions imposed by 18 U.S.C. § 641. Section 641 provides, in pertinent part, that whoever knowingly converts to their use or the use of another, or without authority, sells, conveys, or disposes of any record of the United States or whoever receives the same with intent to convert it to their use or gain, knowing it to have been converted, shall be guiltyof a crime punishable by a fine of up to $10,000.00 or imprisoned up to ten (10) years, or both.

3. Facility Security Requirements

It is expected that all work will be performed at the Government (DEA) site, or through approved telework means. However, any DEA work that is performed at the Contractor's facility must be protected by an approved security file container that conforms to Federal specifications and bears a"Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock. Such containers must be labeled "General Services Administration Approved Security Container" on the face of the top drawer.

The Contractor shall be responsible for physically safeguarding all Government (DEA) records inits possession, including records in the possession of the Contractor personnel, from theft, tampering, misuse, etc.

B. REMOVAL FROM THE CONTRACT

At the direction of the Contracting Officer, the Contractor is required to immediately remove any Contractor Personnel from work under the Contract should it be determined by DEA that such a person has been determined to be unsuitable or ineligible to work under the Contract for any of the following reasons: violation of the Contractor Responsibilities or any performance standard or requirement described in the Contract; disqualification for either suitability or security reasons (including DEA's Drug Use Policy); lack of fitness for the performance of duties when continued work under the Contract may jeopardize, compromise, or disrupt the safety and security of DEA facilities, property, information, and operations; presenting an actual or potential threat of any kind to DEA/DOJ employees, official visitors, or the visiting public; or whose continued work under the Contract is otherwise contrary to the public interest as determined by the Contracting Officer.

The Contractor and its personnel agree that DEA may immediately and without advance notice, remove Contractor Personnel from a DEA worksite or release him/her from their contractual duties for failing or refusingto perform any duty under the Contract or failing to cooperate fully with any inquiry pertaining to the Contract.In addition, DEA reserves the right to take any and all relief appropriate under the circumstances. In the event that any such action is taken, neither the Contractor nor its personnel are entitled to be informed of the basis for theaction. Such notice is within the sole discretion of DEA. In these instances, neither the Contractor nor its personnel will be entitled to any compensation for DEA's actions. Any costs incurred by the Contractor for removal of a Contractor Personnel from work under the Contract and any costs incurred in the replacement, including, but limited to, costs for recruiting, training, certifying, clearing, and otherwise qualifying replacement personnel, travel, or litigation are not reimbursable to the Contractor.

The Contracting Officer will notify the Contractor orally or in writing of the need to remove or the removal of any person from performance of work under the Contract. Oral notification will be confirmed in writing by theContracting Officer. Removals may be effective for a temporary period or permanently, as directed by the Contracting Officer. **The Contracting Officer's determination to permanently remove a person from workunder the Contract will be final**. If the Contractor is notified that a Contractor Personnel's access to DEA hasbeen revoked or suspended, the Contractor must remove the Contractor Personnel immediately from further performance of services for DEA. The Contractor must also collect and return any DEA property.

II. CONTRACTOR PERSONNEL RESPONSIBILITIES

Contractor Personnel who perform work under the Contract agree to comply with the *standards* set forth in this document. These requirements cover conduct onand off duty, unless otherwise noted. The standards include, but are not limited to:

A. MINIMUM STANDARDS OF CONDUCT IN PERFORMANCE OF DUTIES:

1. Conduct

a. Contractor personnel shall maintain a business-like appearance at all times while on official duty in a government-owned or leased property (government facility). Except when authorized by the COR to use another mode of dress because of the need to perform a special task or for other circumstances (e.g., placing retired files in boxes), the standard of dress is "business casual";

b. Contractor personnel shall remain alert at all times while on duty;

c. Contractor personnel shall not engage or participate in gambling, betting, or

management oflotteries while in a government facility or while performing contract responsibilities;

d. Contractor personnel shall not discuss duty assignment(s) under the Contract, except in an official business capacity with the Contractor's Point of Contact and fellow Contractor Personnel assignedto the Contract, DEA officials, or other Government officials having an official need-to-know;
e. Contractor personnel shall not distribute or disclose information not available to the general publicfor non-official purposes;
f. Contractor personnel shall not access or attempt to access restricted space or property if notauthorized;
g. Contractor personnel shall not take or use any DEA property, material, or information (e.g., DEA building passes, credentials, reports, or files) associated with the performance of work under the Contract for purposes other than performance of work under the Contract;
h. Contractor personnel shall not engage in disorderly conduct, use of abusive or offensivelanguage, quarreling, intimidation by words or actions, or fighting;
i. Contractor personnel shall not use a controlled substance except as maybe prescribed to the employee by a duly licensed medical professional for treatment of illness or condition or as contained in an over-the-counter medication;
j. Contractor personnel shall not consume, possess, or be under the influence of alcoholic beverages orother intoxicants while on duty or while present at a government facility;
k. Contractor personnel shall not solicit or accept gifts, favors, or bribes in connection with theperformance of duties under the Contract;
l. Contractor personnel shall not intentionally destroy, mutilate, remove, falsify, conceal, alter, or makean unauthorized copy of any Government record for his/her own purposes, or conceal material facts by willful omission from official documents or records;
m. Contractor personnel shall not discriminate or sexually harass any person during the performanceof duties under the Contract;
n. Contractor personnel shall refrain from engaging in any criminal, infamous, dishonest, or notoriously disgraceful conduct or other conduct prejudicial to DEA, to DOJ, or to the UnitedStates Government. This includes any conduct that indicates that contractor personnel failed to exercise good judgment either on or off duty. Contractor personnel shall always conduct themselves in a professional manner and observe the DEA Standards of Conduct, as well as applicable orders, policies, regulations, and laws of DEA, DOJ, and the federal government; and
o. Contractor personnel shall not give false or misleading statements, or conceal facts, in connectionwith obtaining or retaining employment under or performing duties under the Contract. This includes, but is not limited to, the provision of information during any administrative or criminal investigation or other proceeding, and the preparation of official reports.

2. Affiliations

a. Contractor personnel are prohibited from associating with individuals known or suspected to be involved in illegal drug trafficking or other criminal activity in other than a strictly professional capacity. Contractor personnel are to strictly maintain only the highest standards of conduct withrespect to informants, known criminals, or with individuals engaged in criminal activity.
b. Contractor personnel may not associate with family members who are engaged in or suspected of engaging in ongoing criminal activity. Occasionally, contractor personnel

may have a family member who has been arrested, charged or convicted for criminal activity. Contractor personnel are not required to sever ties with family members who have committed to a *bona fide* substance abuse recovery program and may assist in the rehabilitative process, with supervisory notification. Nevertheless, contractor personnel are expected to conduct themselves in a manner that is above reproach when interacting with such family members. This includes taking particular care in safeguarding DEA information and avoiding situations where the contractor personnel could be implicated in criminal activity.

c. Contractor personnel are required to immediately inform their supervisor and COR of any instancein which they have reason to believe that a spouse, domestic partner, or dependent child is suspected of committing any felony or any drug-related offense. Similarly, contractor personnel must immediately report to their supervisor and COR any instance in which they have reason to believe that someone residing in the same residence as the contractor personnel, regardless of relationship, is suspected of committing any felony or any drug-related offense.

B. SECURITY REQUIREMENTS

1. Information Security Requirements

a. All work performed under the Contract may require access to one or more of the following categoriesof protected information: Personally Identifiable Information, DEA Sensitive (including, Sensitive But Unclassified, Law Enforcement Sensitive and Controlled Unclassified Information), Secret, Top Secret, or Top Secret with SCI Access. All Contractor Personnel shall comply with all Federal, Department of Justice, and DEA regulations, policies, and guidelines regarding information security, including DEA's Information Technology ("IT") Rules of Behavior and the Freedom of Information and Privacy Act.

b. Prior to the commencement of any work for DEA, Contractor Personnel shall complete a DEA-487,Reporting Responsibilities/Non-Disclosure Agreement. The declaration must be witnessed and may be accepted by a duly authorized DEA representative (generally the COR or a DEA Security Officer).Failure or refusal to complete a DEA-487 is grounds for disqualification as a contractor for suitability/fitness reasons.

c. Unless otherwise expressly stated in the Contract, Contractor Personnel are strictly prohibited from using company or personal computers, thumb drives, storage devices, source media, or other electronic devices to store or process DEA work, data, or other product produced while employed by the DEA. All source materials, information, and resultant work products are the property of DEAand shall not be used by the Contractor for any other purpose. All data received by Contractor Personnel shall be handled, stored, transmitted, reproduced, and destroyed in accordance with DEAprocedures. Upon termination or expiration of a contract, all data (documents and other media) andwork products shall be relinquished immediately to the COR or designated DEA employee.

d. Contractor Personnel shall hold all information obtained under a DEA contract in the strictest confidence. All information obtained shall be used only for the purpose of performing the Contractand shall not be divulged nor made known in any manner to any person except as necessary to perform the Contract. The Contractor Personnel shall not divulge, sell, or distribute any informationat any point in time, even after termination or expiration of a contract.

e. Except as specifically authorized in writing by the COR, Contractor Personnel are prohibited from introducing any form of outside computer media into Government-owned computers or

contractor-supplied computers located in the Government facility.

f. Except as specifically authorized by the COR, Contractor Personnel are prohibited from removing any documents, records, source media, supplies, or equipment from the Government facility.
g. Except as specifically authorized by the COR, Contractor Personnel are prohibited from reproducingDEA source media or written products.
h. Contractor Personnel shall ensure that IT systems are appropriately safeguarded. If new or emerging security threats or hazards are discovered or anticipated by either the Government or the Contractor, or if current security safeguards cease to function, the discoverer shall bring the situation to the attention of the COR immediately.

2. Facility Security Requirements

It is expected that all work will be performed at the Government (DEA) site, or by accessing by DEA telecommunications systems and networks. However, any DEA work that is performed at the Contractor's facility must be protected by an approved security file container that conforms to Federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock. Such containers must be labeled "General Services AdministrationApproved Security Container" on the face of the top drawer.

The Contractor personnel shall be responsible for physically safeguarding all Government (DEA) recordsin its possession, including records in the possession of the Contractor personnel, from theft, tampering,misuse, etc.

The following requirements ensure Compliance with Homeland Security Presidential Directive-12 ("HSPD-12") and Federal Information Processing Standard Publication 201 ("FIPS 201") entitled "Personal Identification Verification ('PIV') for Federal Employees and Contractors."

a. Contractor personnel must appear in person at least once before a DEA official who is responsible for checking the identification documents described in 2.d., below.
b. For Contractor personnel who report for assignment to a DEA contract under a waiver pending completion of the background investigation, the facility access/building pass shall be re-validated byDEA when the background investigation is completed and favorably adjudicated. If the final adjudication is unfavorable for any reason, facility access/building passes badges issued under a waiver will be suspended or revoked.
c. The COR is responsible for collecting all DEA-issued property upon the departure of an individualfrom assignment to the Contract. DEA-issued property includes, but is not limited to: building passes, identification badges, credentials, computers, files (paper or electronic media), and office equipment, supplies and accessories. The COR is responsible for returning the referenced propertyto the appropriate program office after receipt from the contractor.
d. Contractor Personnel must present to DEA two types of identification in original form prior to being issued a facility access/building pass. At least one form of identification shall be a valid state or U.S. Government issued picture ID. The other acceptable types of identification are:

- United States Passport (unexpired or expired)
- Identification Card (issued by a State oroutlying possession of the United States provided it contains a photograph or information such as name, date of birth,sex, height, eye color, and address)
- United States Social Security Card
- United States Military Card or Draft Record
- United States Coast Guard Merchant Mariner Card
- Certificate of United States Citizenship
- Alien Registration Receipt Card
- Unexpired Temporary Resident Card
- Driver's License issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, sex, height, eye color, andaddress
- Voter's Registration Card
- Birth Certificate (original or certified)
- Military Dependent Identification Card
- Native American Tribal Document
- Certificate of Naturalization
- Unexpired Foreign Passport which contains an I-551 stamp
- Unexpired Employment Authorization Card

C. PRIVACY

Contractor Personnel agree that there is no expectation of privacy in any Government (DEA) assigned or controlled work space, including: offices, computers, workstations, closets, or storage facilities. Nor is there any expectation of privacy in any DEA equipment or other asset or fixture, including, but not limitedto: desks, safes, file cabinets or containers of any kind, computers and any storage media, or any such spaces or equipment provided by the Contractor or its personnel for use in DEA facilities or premises.

Contractor Personnel shall be placed on notice that any space or equipment may be searched with orwithout notice to the Contractor and its personnel.

All data located in a DEA computer and/or communication system, including documents, electronic files,emails and recorded voice mail messages are the property of DEA. DEA or its designee may inspect and monitor such data at any time. No individual should have any expectation of privacy in messages, even those messages marked as "private" or other data recorded in DEA's systems. This includes documents ormessages that may have been deleted, but not completely removed from the system.

D. ADMINISTRATIVE INQUIRIES

All Contractor Personnel assigned to, or otherwise participating in the performance of the Contract, agreeto comply with any inspection, investigation, review and/or inquiry of inappropriate conduct and/or allegations of impropriety, whether administrative or criminal in nature, conducted by a duly appointed official of DOJ's Office of the Inspector General, DEA's Office of Professional Responsibility, or DEA'sOffice of Inspections.

All Contractor Personnel agree to cooperate fully and to the best of their ability with any such inspections, investigations, and/or inquiries. In accordance with federal and state law, Contractor Personnel will respondfully and truthfully to all questioning and provide, as required, sworn statements, declarations, or affirmations as directed, or participate in transcribed interviews. Contractor Personnel shall retain their constitutional protection against compelled self-incrimination at all times. However, Contractor Personnel are required to answer questions under the following conditions:

1. The inquiry being conducted will not subject Contractor Personnel to criminal prosecution; and
2. Statements made cannot be used in any criminal prosecution (except in cases where the subject is criminally prosecuted for knowingly and willfully providing false information to investigativepersonnel).

All Contractor Personnel assigned to, or otherwise participating in the performance of the Contract, also agree to comply with any inquiry regarding insider threat detection or security incident detection conductedby a duly appointed official of DEA's Office of Security Programs.

A determination by DEA that a person is not suitable or eligible to perform work under the Contract is not adenial, suspension, or revocation of a previously granted security clearance by another agency, nor shall it be interpreted as a direction or recommendation to the Contractor regarding the suitability or eligibility of the affected individual for employment outside the scope of DEA.

I,_____(Contractor Personnel Printed Name) have read and understood therequirements of the above-listed Contractor Responsibilities and all the documents attached or referenced herein.

_____

Contractor Personnel Signature/Date

SECURITY REQUIREMENTS FOR NON-SENSITIVE POSITIONS ESCORTED ACCESS—
U. S. CITIZENSHIP REQUIRED

DEA's personnel, information, and facility security requirements for contracts, task orders, delivery orders, purchase orders, blanket purchase agreements, reimbursable agreements, and other types of contractual arrangements (hereafter referred to as "contract" and "Contractor") to provide goods and services to DEA are hereby provided for the subject access level. The forms listed in Section V are available at http://www.dea.gov. Click on Acquisitions & Contracts and go to Security Forms.

I. GENERAL

A. Contractor's Security Officer

1. The Contractor shall establish and maintain a security program to ensure that all requirements set forth in this provision are accomplished efficiently and effectively. The Contractor's time and expenses for recruiting, interviewing, and security screening are considered overhead and may not be billed directly to DEA.

2. The Contractor shall designate a Security Officer, and an Alternate Security Officer in case of the primary Security Officer's absence, with the authority and responsibility to perform personnel security screening to the extent possible.

3. The Contractor shall make every effort to preclude incurrence of avoidable costs by the Government by ensuring that all applicants and personnel furnished on this contract are eligible, reliable, and of reputable background and sound character. Security screening shall include, but not be limited to, verification of current home address, telephone number, and prior work experience (See Item 8 under D. Documentation Requirements below.), and resolution of delinquent debt related issues that have the potential to disqualify an applicant from consideration for employment on a DEA contract.

4. The Contractor shall ensure that applicants submitted to DEA meet the basic eligibility requirements, such as job skills, certificates if required, residency, and none of the disqualifying factors described below. DEA recognizes that law enforcement records and other information the Contractor is able to obtain regarding an individual's history relative to the disqualifying factors is limited. However, much of this information is requested on Standard Form 85, Questionnaire for Non-Sensitive Positions (Revised November 2021). The Contractor is encouraged to re-interview each applicant based on the answers entered on the SF85.

5. Debt-related issues are the most prevalent derogatory issues found during background investigations and cause delays in the adjudication of security clearances. The Contractor is encouraged to obtain the applicant/employee's credit report and have any issues resolved prior to submitting the security clearance request forms to DEA. DEA currently uses Equifax Credit Reporting Services; however, the Contractor may use the credit reporting agency of its choice. In compliance with the Fair Credit Reporting Act of 1970, as amended (15 U.S.C. 1681, *et seq.)*, the following must be used when the Contractor obtains a credit report:

a. A credit report shall be obtained for accounts in the applicant/employee's name only. This will be a "personal report for employment purposes." *Do not obtain a credit report for joint accounts.*

b. The Contractor shall provide a written notice/release to the applicant/employee that a credit report may be used for employment purposes. The applicant/employee shall sign and date the notice/release and provide it to the Contractor before the credit report is obtained by the Contractor. The Contractor is not authorized to obtain a credit report prior to receipt of the signed notice/release. This signed notice/release is required in addition to the form DOJ-555, Disclosure and Authorization Pertaining to Consumer Reports, Pursuant to the Fair Credit Reporting Act. A copy of the signed notice/release shall be submitted to DEA with the DOJ-555.

c. The Contractor shall not take adverse action against the applicant/employee, based in whole or in part upon the credit report, without first providing the applicant/employee a copy of the credit report and a written description of the applicant/employee's rights as described under Section 1681g(c)(3) of Title 15 U.S.C.

d. If a potentially disqualifying debt-related issue surfaces that the applicant/employee omitted from the SF85, Questionnaire for Non-Sensitive Positions, the personnel security request forms should not be submitted to DEA unless the applicant/employee provides strong mitigating information that clearly explains the omission and how the issue will be satisfactorily resolved.

e. Blank forms and additional information regarding credit reports are available at http://www.dea.gov; click on Security Forms.

6. The Contractor shall ensure that all security related forms and questionnaires are filled out correctly and completely and are signed, dated, and submitted to the Contracting Officer's Technical Representative or Task Monitor (COTR/TM) in a timely manner. *Personnel security packages with incomplete documentation may be rejected and returned to the contactor without any further actions performed by DEA.*

7. DEA's request for additional information or documents regarding the background inquiries shall be responded to within 30 days unless the COTR/TM provides a written extension. *Failure to submit the requested information or documents in a timely manner may result in the applicant being determined unreliable and unsuitable for employment on a DEA contract.*

8. The monthly Administrative Report shall include the status of the Contractor's applicants seeking DEA security approvals. The report shall contain the current status of all personnel security requests, to include: Dates the packages were submitted to the COTR/TM; dates security approval notifications were received from DEA; the number of approved employees; the number of disapproved applicants; and the number of applicants pending approval. The due date of the report will be established by the COTR/TM upon contract award or the issuance of an order.

B. General Requirements

1. DEA will conduct background inquiries on all of the Contractor's personnel to be assigned to this contract and on those officials of the company, *including the Security Officer and Alternate Security Officer,* who will be directly involved in any aspect of management of the assigned personnel.

2. Contractors shall include the following statement in employment advertisements: *"Applicants selected will be subject to a Government security background investigation and must meet eligibility and suitability requirements."*

3. As a minimum, DEA will query law enforcement agencies' indices and the following record systems:

- Fingerprint Query by the Federal Bureau of Investigation (FBI)
- Narcotics and Dangerous Drug Information System (NADDIS)
- National Crime Information Center (NCIC)
- National Law Enforcement Telecommunications System (NLETS)
- Credit Reporting Agencies

4. Only U.S. citizens, by birth or naturalized, shall be permitted to perform services on this contract.

5. All applicants must have resided legally in the United States for at least three (3) years of the last five (5) years, *unless the applicant was*: (The three (3) years do not have to be consecutive.)

- a U.S. Government employee assigned to a U.S. embassy or U.S. consulate in a foreign country;
- a U.S. Government Contractor's employee, who is a U.S. citizen assigned to a U.S. embassy, U.S. consulate, or U.S. military installation in a foreign country, and who is not ordinarily a resident of the country.
- a member of the U.S. armed forces stationed in a foreign country; or
- a dependent family member of a U.S. Government or U.S. armed forces employee assigned overseas.

6. All personnel assigned to this contract must be approved in writing by the DEA Office of Security Programs for escorted access to DEA facilities and worksites.

7. The Contractor's employee(s) shall not be assigned to perform services for DEA until the Contractor has been notified in writing by the COTR/TM that the individual(s) has been approved by the DEA Office of Security Programs.

8. Applicants whose background inquiries result in a determination of unsuitable or are otherwise determined unfavorable based on derogatory information shall be removed from further consideration for performance under this or *any* DEA contract. DEA reserves the right to refuse the services of and/or terminate the access of any Contractor employee or applicant who is or may be judged a security risk. The COTR/TM will inform the Contractor in writing of any objections concerning specific applicants and personnel, but is not permitted to provide specific information due to the Freedom of Information Act and the Privacy Act (FOIA/PA).

9. A determination by DEA that a person is not suitable to perform work under this contract is not a denial, suspension, or revocation of a previously granted security clearance by another agency, nor shall it be interpreted as a direction or recommendation to the Contractor regarding the suitability of an affected individual for employment outside the scope of DEA.

10. The Contractor shall immediately inform the COTR/TM in writing when an employee or applicant for a DEA contract has transferred to another contract, has resigned, or has been terminated by the Contractor, or any other type of action that constitutes a break in the Contractor-employee relationship. The COTR/TM shall provide such information in writing to the DEA Office of Security Programs, Personnel Security Section (ISR).

11. The COTR/TM shall be the Contractor's point of contact for all personnel security communications, inquiries, and issues regarding this contract. All required documents must be submitted by the Contractor to the COTR/TM. The COTR/TM will not communicate directly with the Contractor's employees or applicants regarding personnel security issues unless communicating through the Contractor would violate the FOI/PA.

C. Documentation Requirements

1. A clearance for access to national security information (NSI) is not required nor authorized by this contract. However, a previously conducted background investigation that was favorably adjudicated by the Department of Defense (DOD) and considered to be current will be accepted and supplemented with criminal record and credit report checks conducted by DEA. *The Contractor's transmittal letter to DEA must indicate the applicant has a security clearance through DOD.*

1.a. Only those forms described below in Items 1.b; 1.c; 1.d; 5; 8; 10; and 11 (16 and 17 if applicable) are required to be submitted to the COTR/TM when the applicant has current NSI clearance through DOD.

1.b. One (1) original of form, Contract Employee's Authorization to Conduct Agency-Specific Record Checks (February 2009). This will be used by DEA to supplement the criminal record checks previously conducted by the DOD.

1.c. One (1) copy of the DISS Personnel Summary if the applicant has a CONFIDENTIAL, SECRET or TOP SECRET NSI clearance granted through the DOD. A DISS Personnel Summary is considered current as follows and is based on the investigation date. It is **NOT** based on the date the clearance was granted by DOD or the date the DISS Personnel Summary was issued to the contractor:

- CONFIDENTIAL – Date of the background investigation or periodic reinvestigation is not more than fifteen (15) years ago.
- SECRET – Date of the background investigation or periodic reinvestigation is not more than ten (10) years ago.
- TOP SECRET – Date of the background investigation or periodic reinvestigation is not more than five (5) years ago.

2.d. A DISS Personne Summary that states an INTERIM clearance will be accepted when the date the INTERIM clearance was granted was not more than one (1) year from the date of submission to DEA. A copy of the final clearance shall be provided to the COTR/TM upon receipt. *The COTR/TM shall forward the final clearance to DEA Headquarters/Personnel Security Section.* (Because access to NSI is not required nor authorized by this contract, the DISS Personnel Summary does not have to show the providing Contractor's organizational name as the clearance holder.)

1.e. *Do not submit a DISS Personnel Summary that states*: Loss of Jurisdiction, Declination, Discontinued, Cancelled, Denied, Revoked, Suspended, or any other terminology which indicates the applicant does not have a current clearance or current clearance eligibility.

1.f. F86, Questionnaire for National Security Positions; SF85P Questionnaire for Public Trust Positions; SF85P-S, Supplemental Questionnaire for Selected Positions; SF85, Questionnaire for Non-Sensitive Positions; Fingerprint cards; OBD-236, Inquiry Regarding Suitability of Applicant; Loyalty Oath; Foreign National Relatives or Associates Statement; and Verification of U.S. Citizenship forms are **NOT** required when the applicant has a current DOD clearance and DISS Personnel Summary is provided.

2. **If the applicant has a favorable Public Trust Suitability Determination by another U. S. Government agency**, provide one (1) copy of that agency's Notice of Suitability Determination. The Notice must indicate the type of background investigation and the date it was completed. The background investigation must have been completed no longer than five (5) years prior to the date it is verified by DEA.

2.a. OBD-236, Inquiry Regarding Suitability of Applicant; Loyalty Oath; Foreign National Relatives or Associates Statement; and Verification of U.S. Citizenship forms are **NOT** required when the applicant has a favorable Public Trust Suitability Determination by another U.S. Government agency. One (1) copy of the SF85, Questionnaire for Non-Sensitive Positions **IS** required.

3.The forms and documents described in Items 5 through 17 below shall be completed and submitted as instructed for each form and submitted to the COTR/TM. The COTR/TM will provide a supply of blank fingerprint cards to the Contractor. The Contractor shall reproduce the other forms listed below under Section V. SECURITY FORMS as needed. The completed forms will be used by DEA to conduct the background inquiries or to supplement a background investigation previously conducted by DOD or other U.S. Government agency. DO NOT SUBMIT FORMS AND DOCUMENTS THAT ARE NOT REQUIRED. DO NOT SUBMIT EXTRA COPIES OF FORMS.

4.Do not staple or use ACCO fasteners or otherwise bind the forms together. A paper clip or binder clip will suffice. Put each applicant's forms in a separate envelope with the name of the Contractor, contract number, and the applicant's full name and labor category on the front of the envelope. Submit the completed forms to the COTR/TM at the address provided elsewhere in this contract via hand delivery, FedEx, UPS, Express Mail, Registered Mail, Delivery Confirmation, etc., to have a record of delivery and receipt.

5.One (1) original and separate transmittal letter on official company stationery for each applicant which indicates the contract/order/agreement number, the applicant's full name, social security number, and labor category.

6.One (1) original of form SF85, entitled Questionnaire for Non-Sensitive Positions (Revised November 2021), with original signatures in black ink on Page 5 and the Authorization for Release of Medical Information. The SF85P may be typed or legibly printed by hand. *DO NOT SUBMIT THE INSTRUCTION PAGES OF THE SF85. (An SF85 is not required if the applicant possesses a current CONFIDENTIAL, SECRET, or TOP SECRET security clearance—or an interim clearance—granted by DOD or another U. S. Government agency. Submit the* Contract Employee's Authorization to Conduct Agency-Specific Record Checks *form instead.)*

6.a. All white-outs, erasures, or other types of corrections or changes on the SF85 must be initialed by the applicant.

6.b. The date of the applicant's signature on the SF85 must not be more than 30 days old when submitted to the COTR/TM. Pen and ink changes, with the applicant's initials, or supplemental information on a plain piece of paper with the applicant's name, social security number, and signature are acceptable methods to update and correct the SF85. Page 5 and the Authorization for Release of Medical Information must be signed again with a current date. If there are no changes since the date the SF85 was signed originally, the applicant may re-sign and re-date the SF85 with the notation, "No changes."

7. Applicant will make an appointment to be electronically fingerprinted per instructions provided by COR/TM. Upon completion of fingerprinting, fingerprints will be electronically transmitted to DCSA by vendor. Fingerprint results will be transmitted from DCSA to Office of Security Programs, Personnel Security Section (ISR). (*Fingerprints are not required if the applicant possesses a current CONFIDENTIAL, SECRET, or TOP SECRET security clearance—or an interim clearance—granted by DOD or a favorable Public Trust Suitability Determination by another U. S. Government agency.)*

8. One (1) original of the 3-page Drug Use Statement. The witness may be the Contractor's Security Officer, personnel officer, project officer, project manager, vice president, or president or a notary public as long as the witness occupies a position of responsibility and is not a relative of the applicant. *The witness' name and title must be printed under the signature line.*

9. One (1) original of each form OBD-236, Inquiry Regarding Suitability of Applicant (May. 2000), prepared as applicable to 9.a. or 9.b. below. OBD-236 forms may be typed or printed legibly by hand.(*OBD-236 forms are not required if the applicant possesses a current CONFIDENTIAL, SECRET, or TOP SECRET security clearance—or an interim clearance—granted by DOD or a favorable Public Trust Suitability Determination by another U. S. Government agency.)*

9.a. Each employer for the past five (5) years, including the current employer, shall be contacted by telephone and asked all eight (8) questions—and only those questions—on the OBD-236. Verified dates of employment will be accepted if an employer's corporate policy does not permit providing additional information. If an employer cannot be contacted, efforts to make contact shall be noted on the OBD-236.

9.b. If the applicant does not have an employment history, three (3) associates/references shall be contacted by telephone and asked questions 1 through 5—and only those questions—on the OBD-236. The references must have known the applicant for at least two (2) years and may be co-workers, personal references, or selected from the names provided in Questions 8 and 9 of the SF85.

10. One (1) original of Department of Justice Form DOJ-555 (Revised Oct. 2008), Disclosure and Authorization Pertaining to Consumer Reports, Pursuant to the Fair Credit Reporting Act. The "Current Organization Assigned" is the Contractor's corporate name plus the DEA Division/Office for this contract.

11. One (1) original of the form entitled, RELEASE—FAIR CREDIT REPORTING ACT OF 1970, AS AMENDED. This form is required in addition to the DOJ-555 above.

12. *If applicable,* one (1) original of Loyalty Oath: Only if the applicant is a U.S. citizen, by birth or naturalized, and has *dual citizenship* in a foreign country.

13. *If applicable,* one (1) original of Foreign National Relatives or Associates Statement: Only if the applicant has *foreign national relatives or associates*, regardless of whether the foreign national relatives or associates reside in the United States or a foreign country. Do not include foreign-born relatives or associates who are United States citizens. Once a foreign-born individual acquires United States citizenship, the individual is no longer a "foreign national."

14. *If applicable,* one (1) copy of the U.S. Citizenship Certificate of Naturalization or U. S. Passport. This may be either a current or previous U. S. Passport. NOTE: The National Industrial Security Program Operating Manual, DOD Directive 5520.22-M, Section 2-206, authorizes the Contractor to require each applicant who claims U.S. citizenship to produce evidence of citizenship. However, some naturalized U.S. citizens may be reluctant to photocopy the Certificate of Naturalization or U. S. Passport due to the prohibition printed on the front of the certificate. In those cases, an official of the Contractor company or a DEA employee may personally view the Certificate of Naturalization or U. S. Passport and sign a statement verifying that the individual is a U.S. citizen. (A sample statement is provided under Security Forms.)

15. *If applicable,* one (1) copy of a U.S. Department of State form FS-240, FS-545, or DS-1350, Report of Birth Abroad of a Citizen of the United States, or a Certificate of Citizenship: Only if U.S. citizenship was acquired by birth abroad to a U.S. citizen parent or parents.

16. *If applicable,* one (1) copy of the Declaration and one (1) copy of the Trustee's most recent quarterly payment statement or completion of repayment if the applicant filed bankruptcy under Chapter 13 within the past ten years, or one (1) copy of the Order discharging the debt if the applicant filed bankruptcy under Chapter 7 within the past ten years.

17. *If applicable,* one (1) copy of any other document(s) as proof of satisfactorily resolving a delinquent debt issue(s).

E. Disqualifying Factors

Issues may surface concerning security approval or retention of a Contractor's applicant or employee that are not addressed in this contract. If there is any doubt regarding the suitability of an applicant or employee, the individual will not be approved for assignment to this or any DEA contract.

1. **Suitability** is a requirement for employment on a DEA contract as it concerns an individual's conduct, character, reputation, reliability, trustworthiness, loyalty to the United States, and fitness as related to the efficiency of the service. To be suitable, an individual's assignment or continued assignment to a DEA contract must be reasonably expected to promote the efficiency of the DEA's service to the public. A reasonable expectation that an individual's assignment to a DEA contract will not promote the efficiency of the service is established when an adverse connection, or nexus, is shown between the conduct in question and the performance of the individual or DEA accomplishing its mission.

2. Any one or more of the following factors—as disclosed on the SF85P+SF85P-S, in a personal interview with the applicant, or as part of the background investigation—are grounds for **mandatory disqualification** for assignment on a DEA contract and from further consideration for any type of assignment or employment involving DEA. The Contractor is responsible for interviewing each applicant and reviewing the completed security forms using the following criteria. If relevant information obtained is determined to be a **mandatory disqualification factor**, a request for security approval should not be submitted to DEA until the disqualifying factor is resolved favorably.

a. Criminal Record

(1) Conviction resulting from a felony charge(s), regardless of when the conviction occurred.
(2) Multiple misdemeanor convictions, regardless of when the convictions occurred.

(3) Pending indictments or pending criminal charges, regardless of whether the charge(s) is a felony or misdemeanor.
(4) Currently serving a period of probation resulting from a criminal conviction, regardless of whether the conviction is for a felony or a misdemeanor charge.

b. Illegal Drug Use

(1) DEA's mission is to enforce the Controlled Substances Act, 21 USC 801 *et seq.* The illegal use of drugs by any of its personnel, including contractor personnel, may adversely affect the performance of its mission, create a danger to the public safety, expose the agency to civil liability, jeopardize criminal investigations and prosecutions, lead to corruption, or undermine public confidence. Because of its law enforcement responsibilities and the sensitive nature of its work, DEA has a compelling obligation to ensure a workplace that is free of illegal drugs.
(2) Applicants who are found, through investigation or personal admission, to have experimented with or used narcotics or dangerous drugs, except those medically prescribed, possibly may be disqualified for employment on a DEA contract. Disclosed drug use will be decided on a case-by-case basis. *Experimental use or use of any narcotic or dangerous drug, including marijuana, except medically prescribed, after employment on a DEA contract is cause for removal.*

c. False Statements

(1) A false statement is the deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form or interview used to conduct investigations, determine employment qualifications, award benefits or status, such as:
(2) Altering the condition of discharge on military documents.
(3) Altering college transcripts.
(4) Falsely completing or failure to disclose information on the SF-86 or any other documents used in the background investigation process.
(5) Conflicting statements of drug use, either on the SF-86, on the Drug Use Statement, or during the background investigation.

d. Debt Related Issues

(1) The terms indebtedness, delinquent debt, and debt related issues mean lawful financial obligations that are just debts that are past due. Debt related issues raise of number of suitability and security concerns that an individual must satisfactorily resolve before an affirmative adjudicative decision can be made.
(2) Each applicant's indebtedness will be reviewed on an individual basis.
(3) Court imposed judgments, defaulted student loans, and other delinquent financial obligations imposed by law (e.g., child support payments, Federal, state, or local taxes) are matters of serious concern. *The mandatory disqualification policy applies to those applicants who cannot satisfactorily document their efforts to repay student loans or to pay child support, taxes, or judgments.*

e. Allegiance to the United States

(1) Evidence of activities developed during the background investigation that would bring the applicant's allegiance to the United States into question, such as:
(2) Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means.
(3) Foreign influence or preference.

f. Personal Conduct

(1) Evidence of any of the following activities developed during the background investigation relative to the applicant's conduct and integrity.
(2) Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances.
(3) Infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion. *Sexual behavior is a concern if it involves a criminal offense, indicates a personality disorder or emotional disorder, subjects the applicant to coercion, exploitation, or duress, or reflects lack of judgment or discretion. Sexual orientation or preference may not be used as a basis for, or a disqualifying factor in, determining a person's suitability*.
(4) Illness, including any mental condition, the nature of which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case.
(5) Any facts which furnish reason to believe that the applicant may be subjected to coercion, influence, or pressure which may cause him/her to act contrary to the best interest of DEA.
(6) Association with persons involved in criminal activity.
(7) Current or recent history of continuing alcohol or prescription abuse.
(8). Misuse of information technology systems.

F. <u>Personnel Security Requirements</u>

1. When the Contractor's employee reports for duty on a DEA contract, the COTR/TM will provide a DEA Form 487 entitled, Reporting Responsibilities/NonDisclosure Agreement, to the employee and obtain the employee's signature prior to the commencement of services: *This form must be witnessed and signed by a DEA employee.* (See Item 2 under G. <u>Information Security Requirements</u> below.)

2. The Contractor shall notify the COTR/TM in writing of the following, prior to occurrence or immediately thereafter, when a Contractor employee has a change in marital status. The COTR/TM will notify ISR.

a. Married, divorced, or widowed.
b. Date, city, and country of marriage, divorce, or death of spouse.
c. Full name of current or former spouse (if notifying of a marriage, include wife's maiden name and any former married names(s)).
d. New spouse's social security number, date of birth, and place of birth (city, state, and country).
e. New spouse's citizenship (include as applicable: alien registration number, date and place of entry into the United States, date and place of naturalization including courthouse and complete address, and citizenship certificate number).

3. A mandatory periodic reinvestigation will be conducted once every five (5) years if the previous background investigation was based on the SF85P and SF85PS, Questionnaires for Public Trust Positions. A mandatory periodic reinvestigation will be conducted once every fifteen (15) years if the previous background investigation was based on the SF86, Questionnaire for National Security Positions.

Additionally, a reinvestigation will be required for individuals who have not been assigned to a DEA contract for a period of one (1) or more years. The same suitability and security standards that are required for new applicants apply to reinvestigations.

4. If the Contractor is notified that an employee's access to DEA has been revoked or suspended, the Contractor must remove the employee immediately from further performance of services for DEA.

G. Information Security Requirements

1. Work performed under this contract requires access to one or more of the following categories of protected information: DEA SENSITIVE, Sensitive But Unclassified, Law Enforcement Sensitive, or the Freedom of Information Act and Privacy Act. The contractor and its personnel shall comply with all Federal, Department of Justice, and DEA regulations, policies, and guidelines regarding information security.

2. Prior to the commencement of any work for DEA, the contractor's employee(s) shall declare in writing (utilizing form DEA-487, Reporting Responsibilities/NonDisclosure Agreement, described above in Paragraph E-1a) that he or she intends to be governed by and comply with Federal laws prohibiting the disclosure of information obtained during the course of their work for DEA. The declaration will be witnessed and accepted by a duly authorized DEA representative (generally the COTR/TM or a DEA Security Officer) on behalf of the Administrator, DEA.

3. All source materials, information, and resultant work products are the property of DEA and shall not be used by the contractor for any other purpose. All data received by the Contractor and its employees shall be handled, stored, transmitted, reproduced, and destroyed in accordance with DEA procedures. Upon termination or expiration of a contract, all data (documents and other media) and work products shall be relinquished immediately to the COTR/TM.

4. The contractor and its personnel shall hold all information obtained under a DEA contract in the strictest confidence. All information obtained shall be used only for the purpose of performing this contract and shall not be divulged nor made known in any manner to any person except as necessary to perform this contract. The contractor's employee(s) shall not divulge, sell, or distribute any information at any point in time, even after termination or expiration of a contract.

5. Except as specifically authorized in writing by the COTR/TM, the Contractor's personnel are prohibited from bringing any form of outside computer media into the Government (DEA) facility and introducing it onto Government-owned computers or contractor-supplied computers located in the Government facility.

6. Except as specifically authorized by the COTR/TM, the Contractor's personnel are prohibited from removing any documents, records, source media, supplies, or equipment from the Government facility.

7. Except as specifically authorized by the COTR/TM, the Contractor's personnel are prohibited from reproducing DEA source media or written products.

8. The contractor shall notify each of its officers and employees having access to DEA information that such information may be used only for the purpose and to the extent authorized in this contract, and that disclosure of any information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 USC 641. 18 USC 641 provides, in pertinent part, that whoever knowingly converts to their use or the use of another, or without authority, sells, conveys, or disposes of any record of the United States or whoever receives the same with intent to convert it to their use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine of up to $10,000.00 or imprisoned up to ten (10) years, or both.

9. The contractor and its employees shall ensure that information technology (IT) systems are appropriately safeguarded. If new or emerging security threats or hazards are discovered or anticipated by either the Government or the contractor, or if existing security safeguards cease to function, the discoverer shall bring the situation to the attention of the other party immediately.

H. Facility Security Requirements

1. The Contractor's personnel must be escorted by a DEA employee at all time when visiting a DEA or other U. S. Government facility in the performance of this contract.

2. Any DEA work that is performed at the Contractor's facility must be protected by an approved security file container that conforms to Federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock. Such containers must be labeled "General Services Administration Approved Security Container" on the face of the top drawer.

3. The Contractor shall be responsible for physically safeguarding all Government (DEA) records in its possession, including records in the possession of the Contractor's personnel, from theft, tampering, or misuse.

4. The COTR/TM is responsible for collecting all DEA-issued property upon the departure of an individual from assignment to this contract. DEA-issued property includes, but is not limited to: Building Passes, Identification Badges, Credentials, Computers, Files (paper or electronic media), and Office Equipment, Supplies and Accessories.

II. STANDARDS OF CONDUCT

A. The Contractor shall be responsible for maintaining satisfactory standards of employee competence, conduct, appearance, and integrity and shall be responsible for reporting allegations of misconduct to the COTR/TM.

B. All of the Contractor's employees performing work under this contract are required to comply with the following *minimum* standards of conduct:

1. Demonstrate good manners and courtesy toward DEA employees, Federal officials, and the general public, and maintain a respectful and helpful attitude during the performance of duties under this contract.
2. Maintain a neat, well-groomed, and business-like appearance at all times while on official duty. Except when authorized by the COTR/TM to use another mode of dress because of the need to perform a special task or for other circumstance (e.g., placing retired files in boxes), the standard of dress is "business casual" as follows: Male employees shall wear dress shirts and dress slacks (or uniforms when required by the contract/order). Female employees shall wear conservative dresses, dress slacks or skirts and sweaters or blouses (or uniforms when required by the contract/order).

3. On or off duty, do not discuss DEA internal matters, policies, grievances, or personalities. Do not discuss financial, personal, or family matters with DEA employees, their family members, or the general public while on duty.
4. On or off duty, do not disclose any official information, except to DEA or other Government officials having an official need-to-know, nor speak to the press on or off the record or issue news or press releases without the express permission of the Contracting Officer.
5. On or off duty, do not discuss duty assignment(s) under this contract except in an official business capacity with the Contractor's Site Supervisor and fellow The Contractor's personnel assigned to this contract, DEA officials, or other Government officials having an official need-to-know.
6. While on duty, do not gamble, unlawfully bet, or promote gambling on Government property or while performing Government work at the Contractor's site.
7. Do not possess or consume narcotics, dangerous drugs, marijuana or other controlled substances while on or off duty, except to the extent that the substance is lawfully prescribed by a licensed medical provider.
8. Abstain from the consumption and possession of alcoholic beverages or other intoxicants while on duty and habitual intoxication while off duty.
9. Remain alert at all times while on duty. Perform assignments in accordance with prescribed laws, regulations, and the terms and conditions of this contract to the best of ability and in accordance with safe and secure working procedures and practices.
10. On or off duty, do not solicit or accept gifts, favors or bribes in connection with the performance of duties under this contract. Report all efforts by others who offer such gifts, favors or bribes to the Contractor's Site Supervisor and to the COTR/TM.
11. On or off duty, do not use any DEA property, material, or information (e.g., DEA building pass or other credentials; DEA reports and files) associated with the performance of work under this contract for purposes other than performance of work under this contract.
12. On or off duty, refrain from any activity that would adversely affect the reputation of the DEA.
13. Neither discriminate against nor sexually harass any person during the performance of duties under this contract.
14. On or off duty, avoid personal and business associations with persons known to be convicted felons or persons known to be connected with criminal activities.
15. On or off duty, do not engage in criminal, infamous, dishonest, immoral, or disgraceful conduct.
16. Ensure that all financial obligations are met.
17. On or off duty, do not give false or misleading statements, or conceal facts, in connection with obtaining or retaining employment under or performing duties under this contract. This includes, but is not limited to, the provision of information during any administrative or criminal investigation or other proceeding, the preparation of travel vouchers, and the preparation of official reports.
18. Do not make statements about fellow employees, DEA officials, their family members, or members of the general public with knowledge of the falseness of the statement or with reckless disregard for the truth.
19. While on duty, do not fail, unnecessarily delay, or refuse to carry out all proper instructions and directions of the Contractor's Site Supervisor or DEA official having oversight responsibility for work under this contract.
20. Do not take, remove, possess, or use Government property or the property of others without written authorization.
21. Do not disturb papers on desks, open desk drawers, cabinets, safes, or enter secure space where access is not authorized.

22. Do not use Government telephones, facsimile, or duplicating equipment except as necessary in the performance of duties under this contract.
23. Do not falsify or unlawfully conceal, remove, mutilate, or destroy any official documents or records, or conceal material facts by willful omission from official documents or records.
24. Do not engage in disorderly conduct, use of abusive or offensive language, quarreling, intimidation by words or actions, or fighting.
25. Do not engage or participate in disruptive activities that interfere with the normal and efficient operations of the Government.

III. REMOVAL FROM WORK

A. The Contractor shall inform its employees of their duties, obligations, and responsibilities under this contract. The Contractor and its employees agree that, in addition to any other actions DEA may be entitled to utilize or employ, any Contractor employees who fail to cooperate fully with any inquiry or investigation or who fail or refuse to perform any duty under this contract may immediately and without advance notice have their DEA access suspended or revoked, be removed from the work site, and be released from their contractual duties. Additionally, DEA reserves the right to take any and all relief appropriate under the circumstances. In the event that any such action is taken, neither the Contractor nor its employees are entitled to be informed of the basis for the action. Such notice is within the sole discretion of DEA. In these instances, neither the Contractor nor its personnel will be entitled to any compensation for DEA's actions.

B. At the direction of the Contracting Officer, the Contractor is required to immediately remove any person from work under this contract should it be determined by DEA that such a person has violated or is in violation of the Standards of Conduct described above or another performance standard or requirement described in this contract; has been disqualified for either suitability or security reasons; who is found to be unfit for the performance of duties; whose continued work under this contract may jeopardize, compromise, or disrupt the safety and security of DEA facilities, property, information, and operations; who presents an actual or potential threat of any kind to DEA employees, official visitors, or the visiting public; or, whose continued work under this contract is otherwise contrary to the public interest as determined by the Contracting Officer.

C. The Contracting Officer will notify the Contractor orally or in writing of the need to remove, or the removal of, any person from performance of work under this contract. Oral notification will be confirmed in writing by the Contracting Officer. Removals may be effective for a temporary period or permanently, as directed by the Contracting Officer. The Contracting Officer's determination to permanently remove a person from work under this contract shall be final. The Government is not obligated to inform either the Contractor or the person removed of the reason for the removal.

D. Any costs incurred by the Contractor for removal of the Contractor's employee from work under this contract and any costs incurred in the replacement—including, but limited to—costs for recruiting, training, certifying, clearing, and otherwise qualifying replacement personnel, travel, or litigation are not reimbursable to the Contractor.

E. *REPEATED*: A determination by DEA that a person is not suitable to perform work under this order is not a denial, suspension, or revocation of a previously granted security clearance by another agency and nor shall it be interpreted as a direction or recommendation to the Contractor regarding the suitability of the affected individual for employment outside the scope of DEA.

IV. ADMINISTRATIVE INQUIRIES

A. The Contractor, its officers, and its employees assigned to, or otherwise participating in the performance of this contract, shall comply with the following ADMINISTRATIVE INQUIRIES provision. The provision authorizes the conduct of appropriate investigations and inquiries by duly appointed personnel conducting examinations, reviews, or investigations into information concerning inappropriate conduct and/or allegations of impropriety, whether such conduct is criminal or administrative in nature.

B. The Contractor shall obtain, and make available upon request by the Contracting Officer, a certification, signed by each contract employee participating in the performance of this contract, attesting to the fact that they have been apprised of and will comply with the ADMINISTRATIVE INQUIRIES provision as stated herein.

1. The Drug Enforcement Administration (DEA) is a Federal law enforcement agency charged with investigating and prosecuting persons violating the drug laws of the United States. To ensure the public has the highest degree of confidence in the integrity, operations and activities of the DEA, it is essential that the personnel assigned to or employed by Contractors that support DEA conduct themselves appropriately and in accordance with applicable law and regulation.

2. The Contractor and its personnel agree that an inspector or investigator of the DEA, Department of Justice, or any other duly authorized organization or entity shall have the right to conduct any and all inquiries or investigations deemed appropriate by such organizations or entities in response to information concerning, or allegations about, improper conduct or inappropriate actions, whether such conduct is criminal or administrative in nature.

3. The Contractor and its personnel agree to cooperate fully and to the best of their ability with any such inquiries or investigations. The Contractor and its personnel agree that persons performing such investigations or inquiries have the right to question the Contractor's personnel. The Contractor's personnel will respond fully and truthfully to such questioning and provide, as required, sworn statements, declarations, or affirmations, as directed, or participate in transcribed interviews as directed.

4. Contract personnel will retain their constitutional protection against compelled self -incrimination at all times. However, contract employees are required to answer questions under the following conditions: (1) if the subject being questioned is informed that the inquiry being conducted will not subject them to criminal prosecution, and (2) that any statements made by the subject cannot be used against the subject in any criminal prosecution (except in cases where the subject is criminally prosecuted for knowingly and willfully providing false information to investigating personnel). When these conditions are met, the subject is required to respond to questioning in accordance with this provision.

5. The Contractor and its personnel agree that there is no expectation of privacy in any DEA assigned or controlled work space, including offices, workstations, closets, or storage facilities, nor is there any expectation of privacy in any equipment or other asset or fixture including but not limited to desks, safes, file cabinets or containers of any kind, computers and any storage media, or any such spaces or equipment provided by the Contractor or its personnel for use in DEA facilities or premises. The Contractor's personnel shall be placed on notice that any space or equipment may be searched with or without notice to the Contractor and its personnel.

6. The Contractor shall inform its employees of their duties, obligations, and responsibilities under this contract. The Contractor and its personnel agree that, in addition to any other actions DEA may be

entitled to utilize or employ, contract personnel who fail to cooperate fully with any inquiry or who fail or refuse to perform any duty under this contract, may immediately and without advance notice have their DEA clearance suspended or revoked, be removed from the work site, or be released from their contractual duties. In addition, DEA reserves the right to take any and all relief appropriate under the circumstances. In the event that any such action is taken, neither the Contractor nor its personnel are entitled to be informed of the basis for the action. Such notice is within the sole discretion of DEA. In these instances, neither the Contractor nor its personnel will be entitled to any compensation for DEA's actions.

V. SECURITY FORMS

The Contractor does not have permission to alter any of these forms or to convert the forms to corporate letterhead. No other versions of these forms may be used.

- SF85, Questionnaire for Non-Sensitive Positions (Revised November 2021) *(The SF85 is available at http://www.opm.gov; click on Forms; click on Standard Forms; scroll down to SF85. The SF85 may be completed on-line and printed using the OPM Standard Forms link, but cannot be saved or transmitted in electronic format. Blank forms only may be printed from the DEA website.)*

The following forms are available at http://www.dea.gov only; click on Security Forms to print blank forms.

- Three-Page Drug Use Statement
- OBD-236, Inquiry Regarding Suitability of Applicant
- DOJ-555 Revised Oct. 2008, Disclosure and Authorization Pertaining to Consumer Reports, Pursuant to the Fair Credit Reporting Act
- RELEASE—FAIR CREDIT REPORTING ACT OF 1970, AS AMENDED
- Resolution of Debt-Related Issues (10/28/03)
- Common Language for Consumer Credit
- Rules and Regulations – A Summary of Your Rights under the Fair Credit Reporting Act
- Loyalty Oath
- Foreign National Relatives or Associates Statement
- Verification of U.S. Citizenship
- Contract Employee's Authorization to Conduct Agency-Specific Record Checks