						T							
SOLICITATIO	N/CONTRACT OR TO COMPLE					1. REQUISIT 0011533611		IBER			PAG	E10F	44
2. CONTRACT NO.	011 10 001111 22	3. AWARD/E	FFECTIVE DATE	,	ER NUMBER		5. SOL	ICITATIO	N NUMBER		6. SOLIC	ITATION ISS	UE DATE
W911QY20C010		17-Aug-2	2020				1				t Calls) 8. OFFER DUE DATE/LOCAL T ME		
7. FOR SOLICITATION INFORMATION CALL		a. NAME					b. TEL	EPHONE	NUMBER (No C	collect Calls)	8. OFFE	R DUE DATE	/LOCAL T ME
9. ISSUED BY		CODE	W911QY		10. THIS ACQU	JISITION IS		JNRES	TRICTED OR	X SET ASI	DE:	100 % FOR	! :
W6QK ACC-APG N	IATICK				X SMALL BUS	SINESS			NED SMALL BUS)		
CONTRACTING DI	VISION GREENE AVENUE				NOWALL BOX	SINESS			NESS PROGRAM				
NATICK MA 01760-				HUBZONE BUSINESS		ED\	NOSB			AICS: 25412			
							ш			3	23412		
TEL:					SERVICE-I VETERAN		8(A))			IZE STAN	NDARD:	
FAX: 508-233-57	700				SMALL BU	SINESS		I		1	,250		
11. DELIVERY FOR			UNT TERMS		П120 ТЫС	CONTRACT	TIC A	13b. I	RATING				
TION UNLESS I	BLOCK IS	Net 30 Da	iys		RATE	D ORDER	UNDER		F7100 05 00				
SEE SCHE	DULE				DPAS	6 (15 CFR 7	00)	14. M	ETHOD OF SO		Г	٦	
								<u> L</u>	RFQ	IFB	L	RFP	
15. DELIVER TO		CODE	W56XNH		16. ADMINISTE	ERED BY				C	ODE _		
BARDA (b) (6)													
BIOMEDICAL ADVANC 200 C STREET, SW	ED RESEARCH DEVEL	OPMENT AU	ПН			SEE	ITEN	И 9					
WASHINGTON DC 200	24												
17a.CONTRACTOR	CODE 3GQS9	, ,	ACILITY 3GQS	69	18a. PAYMEN	T WILL BE N	MADE BY	,		С	ODE H	Q0490	
OFFEROR			ODE		DEFENSE FINANCE AND ACCOUNTING SERVICE								
OLOGY BIOSERVION NANOTHERAPEUT	•					DFAS-INDY VP GFEBS							
13200 NW NANO C					8899 E 56TH STREET								
ALACHUA FL 3261					INDIANAPOL	IS IN 46249	9-3800						
TELEPHONE NO.3	386-462-9663 IF REMITTANCE IS	DIFFEDEN	TANDDIT		10h CUDMIT	INN/OICES	TO A DI	DDECC	SHOWN IN B	LOCK 10a	LIMITE	e pi ock	
II I	ESS IN OFFER	DIFFLING	TANDFUT		BELOW IS C				DENDUM	LOCK TOA.	. UNLLS	3 BLOCK	
19.			20.		21. 22. 23. CES QUANTITY UNIT UNIT PRICE AM					24.			
ITEM NO.		SCHEDULI	OF SUPPLIES	/ SERVI	CES		QUAN	IIIIY	UNIT	UNITE	RICE	AIV	OUNT
			SEE SCHE	DULE									
									26. TOTAL	ANN/ADD ANA	OUNT /F	01	0-1-)
25. ACCOUNTING	AND APPROPRIAT	ION DATA							26. TOTAL	AWARD AM	OUNT (F	or Govt. U	se Only)
See Schedul	le										(b)	(4)	
											. ,		
	TION INCORPORA	TEO DV DEI	EDENIOE EAD (2 242 4	F2 242 4 FAD		242 5 4	DE ATT	ACUED A	DDENIDA C	TABE E	TADE NOT	ATTACHED
Zra. SOLICITA	TION INCORPORA	IES DT KEI	ERENCE FAR S)2.212-1.	52.212-4. FAR :	02.212-3. 52	.212-5 A	KE AII	ACHED. AL	DDENDA	ARE	ARE NOT	ATTACHED
27b. CONTRAC	CT/PURCHASE OR	DER INCOR	PORATES BY R	EFEREN	ICE FAR 52.212	-4. FAR 52.	212-5 IS	ATTAC	HED. A	DDENDA	ARE	ARE NOT	ATTACHED
X 28. CONTRAC	TOR IS REQUIRED	TO SIGN 1	HIS DOCUMENT	ΓAND R	ETURN <u>1</u>	ТГ	29. AW	ARD O	F CONTRACT:	REF.			
11^1	SUING OFFICE. CO	ONTRACTOR	R AGREES TO F	URNISH	_		OFFER	DATE	31-Jul-2020	. YOUR	OFFER (ON SOLICI	TATION
1	DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED. (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: SEE SCHEDULE												
ADDITIONAL S	SHEETS SUBJECT I		MS AND CONDI eservation of SARS-CO		PECIFIED.		SETFC	жіпп	EREIN, 13 ACC	EP IED AS	TO HEW	3. SEE 30	HEDULE
30a. SIGNATURE	OF OFFFROR/CO				31a.UNITE	D STATES OF	F AMERIC	CA (SI	GNATURE OF CO	NTRACTING	OFFICER))	
Sa. Sisteriore		(b) (c)	-					, -			_		
		(D) (D)			(h	(6)							
	0					/(-)							
30b. NAME AND T	TITLE OF SIGNER		30c. DATE	SIGNE	31b. NAME	OF CONTRA	CTING O	FFICER	(TYPE (OR PRINT)		31c. DA	TE SIGNED
(TYPE OR PRINT)					(b) (6)	CONTRAC	TING OF	FICER					
(b) (6)			08/17//20		TEL	(b) (6)						17-2	Aug-2020
				EMAI	L: (b) (6								

SOLICITATION OFFER	N/CONTRACT OR TO COMPLE	I 0011533611-0001					E1 OF	44					
2. CONTRACT NO. W911QY20C0101	1	3. AWARD/E	FFECTIVE DATE	4. ORDI	ER NUMBER	•	5. SOL	ICITATIO	ON NUMBER		6. SOLICITATION ISSUE DATE		SUE DATE
7. FOR SOLICITATION INFORMATION CALL		a. NAME		-			b. TELEPHONE NUMBER (No Collect Calls) 8. OFFER I			R DUE DATE	E/LOCAL TIME		
9. ISSUED BY		CODE	W911QY		10. THIS ACQU	JISITION IS	-	JNRES	STRICTED OR	X SET ASII	DE:	100 % FOF	₹:
CONTRACTING DIV	GOK ACC-APG NATICK INTRACTING DIVISION DG 1 GENERAL GREENE AVENUE TICK MA 01760-5011				X SMALL BUSINESS WOMEN-OWNED SMALL BUSINESS (WOSB) ELIG BLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM NAICS: BUSINESS BUSINESS A25412								
TEL:					SERVICE-	DISABLED					IZE STAN	IDABD:	
FAX: 508-233-57	700				VETERAN- SMALL BU		8(A)				,250	NDAND.	
11. DELIVERY FOR TION UNLESS E		12. DISCO Net 30 Da	UNT TERMS			CONTRAC D ORDER		13b.	RATING				
MARKED	NII E					6 (15 CFR 7		14. N	METHOD OF SO		Г	7	
SEE SCHEE	JULE	0005	W56XNH		40. 40.40.40.40.			L	RFQ	IFB		RFP	
15. DELIVER TO BARDA		CODE	MOOVINI		16. ADMINISTE	ERED BY				C	ODE L		
(6) (6) BIOMEDICAL ADVANCI 200 C STREET, SW WASHINGTON DC 2002		OPMENT AU	гн			SEI	EITEN	/ 1 9					
17a.CONTRACTOR	CODE 3GQS	' I	ACILITY 3GQS	S9	18a. PAYMENT WILL BE MADE BY CODE HQ0490								
OLOGY BIOSERVICES, INC NANOTHERAPEUTICS 13200 NW NANO COURT ALACHUA FL 32615-8726 TELEPHONE NO.386-462-9663				DEFENSE FINANCE AND ACCOUNTING SERVICE DFAS-INDY VP GFEBS 8899 E 56TH STREET INDIANAPOLIS IN 46249-3800									
17b. CHECK II SUCH ADDRE	F REMITTANCE IS SS IN OFFER	DIFFEREN	T AND PUT		18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a. UNLESS BLOCK BELOW IS CHECKED X SEE ADDENDUM								
19. ITEM NO.		SCHEDULI	20. OF SUPPLIES	S/ SERVI	CES		I I I			23 UNIT F		1	24. MOUNT
			SEE SCH	EDULE	:								
25. ACCOUNTING	AND APPROPRIAT	TON DATA							26. TOTAL	AWARD AM	OUNT (F	or Govt. U	se Only)
See Schedul	e										(b)	(4)	
닏	TION INCORPORA									DDENDA	ARE]	T ATTACHED
ᆜ	CT/PURCHASE OR					-4. FAR 52	_			DDENDA	ARE	JAKE NOI	T ATTACHED
28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RECOPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH ADELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SP				H AND OFFER DATED 31-Jul-2020 OFFER DATED 31-Jul-2020 VE AND ON ANY (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH AR					HICH ARE				
30a. SIGNATURE OF OFFEROR/CONTRACTOR					31a.UNITE	D STATES (OF AMERIC	CA (S	SIGNATURE OF CO	NTRACTING	OFFICER))	
					(b)	(6)							
30b. NAME AND T	TILE OF SIGNER		30c. DATE	SIGNED	31b. NAME	OF CONTR	ACTING O	FFICER	(TYPE (OR PRINT)		31c. DA	TE SIGNED
(TYPE OR PRINT)						/ CONTRA	CTING OF	FICER				177	Aug-2020
					TEL:							1 1/-	nuy-2020
			1		LIMAI	L: (b) (6)						1	

SOLICITATION/CONTRACT/ORDER FOR C (CONTINUED)				COMMERC	IAL IT	EMS					P.	AGE 2 OF 44
19. ГТЕМ NO.		20. SCHEDULE OF SUPPLIES/ SERVICES				•	21. QUANTIT	γ	22. UNIT	23 UNIT P		24. AMOUNT
TIEM NO.			SEE SCH				QUANIII	Y	ONII	UNITP	RICE	AMOUNI
32a. QUANTITY IN RECEIVED	INSPECTI	ED 🗍	EEN CCEPTED, AND CONF	ORMS TO THE O	CONTRAC	CT. EXCEPT	AS NOTED:					
32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE			•	32c. DATE 32d. PRI			INTED NAME AND TITLE OF AUTHORIZED GOVERNMENT EPRESENTATIVE					
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT R				EPRESENTATIVI	E	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE						
						32g. E-MA	IL OF AUTHORI	ZED G	OVERNMEN	T REPRESE	NTATIVE	Ē
33. SHIP NUMBER	34. FINAL	VOUCH	ER NUMBER	35. AMOUNT VE CORRECT		36.	. PAYMENT	E	PARTIAL	FINAL	37. CHE	ECK NUMBER
38. S/R ACCOUNT	NUMBER	39. S/R	VOUCHER NUMBER	40. PAID BY		1				1		
41a. I CERTIFY THI 41b. SIGNATURE A			RRECT AND PROPER IFYING OFFICER	FOR PAYMENT 41c. DATE	42a. RE	CEIVED BY	(Print)					
					42b. RE	CEIVED AT	(Location)					
					42c. DA	TE REC'D ((YY/MM/DD)	42d. T	OTAL CONT	AINERS		

Section SF 1449 - CONTINUATION SHEET

UNIT PRICE ITEM NO SUPPLIES/SERVICES **QUANTITY** UNIT **AMOUNT** 0001 2 Months Fill and Finish Capacity

FFP

The contractor shall provide the required program management associated with fill and finish capacity reservation for the period beginning (b) (4)

All required work shall be IAW the Statement of Work (SOW) and Commercial Solution Proposal titled Reservation of SARSCOV-2 Fill and Finish Manufacturing Capacity to Support Surge Response dated July 17, 2020, July 31, 2020 and August 10, 2020 respectively.

FOB: Destination PSC CD: 6505

NET AMT

ITEM NO SUPPLIES/SERVICES **QUANTITY UNIT UNIT PRICE AMOUNT** 000101 \$0.00

ACRN AA @(b) (4)

FFP

PURCHASE REQUEST NUMBER: 0011533611-0001

NET AMT \$0.00

ACRN AA CIN: GFEBS001153361100001

Page 4 of 44

ITEM NO SUPPLIES/SERVICES **QUANTITY UNIT UNIT PRICE AMOUNT** 0002 9 Months Fill and Finish Capacity **FFP** The contractor shall provide fill and finish capacity reservation for the period to include program management beginning (b) (4) associated with fill finish reservation. (b) (4) . All required work shall be IAW the SOW and Commercial Solution Proposal titled Reservation of SARSCOV-2 Fill and Finish Manufacturing Capacity to Support Surge Response dated July 17, 2020, July 31, 2020 and August 10, 2020 respectively. The procurement of product or components required for fill is not part of fill and finish capacity. FOB: Destination PSC CD: 6505 **NET AMT** (b) (4) ITEM NO SUPPLIES/SERVICES **QUANTITY UNIT UNIT PRICE AMOUNT** 000201 \$0.00 ACRN AA @ (b) (4) PURCHASE REQUEST NUMBER: 0011533611-0001 **NET AMT** \$0.00 ACRN AA CIN: GFEBS001153361100002

Page 5 of 44

ITEM NO SUPPLIES/SERVICES QUANTITY UNIT UNIT PRICE AMOUNT 0003 12 Months NSP

Technical Data Deliverables

FFP

The contractor shall deliver technical data monthly IAW the contract data deliverables listed Section C.4.1.3. of the Statement of Work (SOW). Data deliverables are due IAW the delivery dates provided in Table 1 within Section C.4.1.2. of the SOW.

FOB: Destination PSC CD: 6505

NET AMT

STATEMENT OF WORK

ADDENDUM: The following pages hereby supplements FAR 52.212-4

SECTION C: STATEMENT of Work (SOW)

TITLE: COVID-19 Fill and Finish Manufacturing Capacity in Support of Operation Warp Speed

- **C.1. Requirement:** The U.S. Army Contracting Command Aberdeen Proving Ground (ACC-APG), Natick Division (Natick) has a requirement to reserve domestic aseptic fill and finish manufacturing capacity for critical vaccines and therapeutics in response to the COVID-19 pandemic in support of Joint Program Executive Office Chemical Biological Radiological Nuclear Defense (JPEO-CBRND), and Health and Human Services (HHS)'s Biomedical Advanced Research and Development Authority (BARDA).
- **C.2. Objective:** BARDA within the Office of the Assistant Secretary for Preparedness and Response (ASPR) at the HHS seeks to identify, retain and secure domestic aseptic fill and finish manufacturing capacity for critical vaccines and therapeutics. BARDA will secure domestic aseptic fill and finish manufacturing capacities to provide uninterrupted supply for a wide-array of vaccines and therapeutics to meet BARDA requirements for the COVID-19 response. BARDA will coordinate the activities as awarded under these contracts.
- **C.3. Background:** In the last twenty years, the U.S. has experienced the destructive effects of both acts of terrorism and infectious disease outbreaks. While limited in scope, the anthrax attacks of 2001 were highly disruptive and suggestive of the impact that large-scale acts of bioterrorism would have, if carried out successfully. Similarly, concerns have escalated that terrorist groups might obtain and use chemical, radiological, and nuclear weapons against civilian populations. Events of the last two decades the SARS epidemic of 2003, the 2009 H1N1 pandemic, the 2014 Ebola epidemic and the on-going (2020) COVID-19 epidemic highlight the persistent threats of emerging infectious diseases.

The Pandemic and All Hazards Preparedness Act (PAHPA) of 2006 established the BARDA to support development and acquisition of Medical Countermeasures (MCMs) to prevent or treat the medical consequences of chemical, biological, radiological, and nuclear (CBRN) threats, pandemic influenza (PI), and emerging infectious diseases (EID). These MCMs include vaccines, therapeutics, diagnostics, and medical devices. Additionally, BARDA is entrusted to foster innovation of technologies that enable better manufacturing, testing, and utilization of these medical countermeasures.

This acquisition is part of a comprehensive strategy and commitment in the BARDA Strategic Plan (2011) to establish assistance to MCM developers directly in the form of technical, clinical and regulatory assistance, and assist BARDA in addressing public health needs in an emergency. To date, BARDA has assisted developers directly in the form of technical, clinical, and regulatory guidance from internal subject matter experts. BARDA established the Centers for Innovation in Advanced Development and Manufacturing (CIADM), Clinical Studies Network (CSN), Nonclinical Studies Network, and the Fill / Finish Manufacturing Network (FFMN) with industry and government partners to assist biological product developers with development, clinical studies and manufacturing. The CIADMs and FFMN were created to rapidly manufacture vaccines and other biological products to address influenza pandemics or emerging infectious disease outbreaks during public health emergencies. BARDA has established the Nonclinical Studies Network and the Clinical Studies Network to provide CBRN MCM developers with animal model and clinical studies.

In December 2019, a novel (new) coronavirus known as SARS-CoV-2 ("the virus") was first detected in Wuhan, Hubei Province, People's Republic of China, causing outbreaks of the coronavirus disease COVID-19 that has now spread globally. HHS declared a public health emergency on January 31, 2020, under section 319 of the Public Health Service Act (42 U.S.C. 247d), in response to COVID-19. On March 1, 2020, the President of the United States, pursuant to sections 01 and 301 of the National Emergencies Act (50 U.S.C. 1601 et seq.) and consistent with section 1135 of the Social Security Act (SSA), as amended (42 U.S.C. 1320b-5), proclaimed that the COVID-19 outbreak in the United States constitutes a national emergency.

As part of the US government's response to the COVID-19 national emergency, BARDA in conjunction with multiple product sponsors is working to develop therapeutics, vaccines and diagnostics to treat, prevent and detect the spread of the SARS-CoV2 virus. Integral to the development of vaccines and biologics is the aseptic fill and finish of these life-saving medical countermeasures.

The 2009 H1N1 influenza pandemic, and influenza vaccine shortages of 2004, illustrated the vulnerability that dependency on offshore manufacturing of pandemic influenza vaccines entails. These events and trends prompted the President and HHS to call for a critical review of the civilian Public Health Emergency Medical Countermeasures Enterprise (PHEMCE). This review, led by the HHS ASPR, resulted in the August 2010 report; The Public Health Emergency Medical Countermeasures Review: Transforming the Enterprise to Meet Long-Range National Needs, that articulated as a strategic imperative that "Current vaccine manufacturers lack the capacity to rapidly "fill and finish" sufficient quantities of pandemic vaccine for the Nation." Typical seasonal vaccine and therapeutic campaigns are scheduled events; where planning and production occur over a five to eight month period and where the demand usually calls for 120-140 million units to be made. In contrast, pandemic events are unpredictable; timeframes are compressed and the sterile injectable product(s) requirements are 3 to 6 times larger.

C.4. Scope of Work: The government seeks to reserve domestic aseptic fill and finish manufacturing capacity for critical vaccines and therapeutics in response to the COVID-19 pandemic to ensure uninterrupted supply throughout the COVID-19 campaign between (b) (4)

. The reserved capacity must include currently unallocated production slots at the specific Contract Manufacturing Organization (CMO) facilities that could be secured for future government use. Included in the "capacity" are the costs associated with facilities and equipment usage for a given production slot, labor, materials as well as support services necessary to fill, label, package, and release a standard batch fill. It is preferred that the offeror provide these services in-house for efficiency and in order to minimize risk. The reservation must exclude the performance of any work in the reserved capacity without explicit, written approval from the government. The offeror must be responsible for management of all activities to meet the goals of the contract, including holding routine meetings with BARDA, and completion of meeting minutes. On a monthly basis, the offeror(s) must provide a monthly report that includes capacity availability and utilization, as well as any issues that affect the operational availability of the reserved capacity.

C.4.1. The strategic objectives of this acquisition are to:

C.4.1.1. Objective 1 – Aseptic Fill and Fill Manufacturing Capacity Reservation and Program Management Requirements:

The offeror will identify domestic aseptic fill and finish manufacturing capacity for critical vaccines and therapeutics in response to the COVID-19 pandemic to ensure uninterrupted supply throughout the COVID-19 campaign to be reserved for the exclusive use of the government for the duration of the period of performance. Where possible, it is preferred that fill and finish activities be completed at the same manufacturing site. The capacity must include currently open production slots on a commercial scale filling line utilizing a multidose vial size (2R, 6R, 10R, etc.), inspection, labeling and packaging, as well as the support services required to release each lot. The offeror(s) must maintain the reserved capacity in a state of readiness and compliance with Food and Drug Administration (FDA) current good manufacturing practices (cGMP), and required Biosafety Level standards as applicable, to perform manufacturing activities, approved by the government, under separate task orders/contracts/agreements for the entirety of the period of performance. The reservation must exclude the performance of any work in the reserved capacity without explicit, written approval from the government. Detailed information for each qualified vial size on their available monthly capacity, batch sizes and estimated run time for that batch. All assumptions required to make these estimations should also be included. For costing purposes, a 10R vial should be specified.

The offeror will be responsible for management of all activities, subcontractors, etc. to meet the goals of the contract, including holding routine meetings with BARDA, and completion of meeting minutes. On a monthly basis, the offeror(s) must provide a monthly report that includes capacity availability and utilization, as well as any issues that affect the operational availability of the reserved capacity.

C.4.1.2. Data Deliverables:

Table 1

No.	Deliverable	Format	Delivery Date
1	Kick-off Meeting	N/A	Within 14 calendar days after award.
2	Risk Management Plan	Electronic copy	Within 30 calendar days after award.
3	Monthly Reports	Electronic copy	15th day of each month
4	Monthly Meetings	Teleconference	Within 5 days of Monthly Report submission.
5	Quarterly Site Visits	Site visit	To be scheduled in coordination with the USG.
6	Ad hoc Site Visits	Site visit	To be scheduled in coordination with the USG.
7	Final Manufacturing Facility Plan	Electronic copy	3 months after contract initiation
8	Security Plan	Electronic copy	2 months after contract initiation
9	Staff increase and training plan	Electronic copy	Within 30 calendar days of contract award.
10	Manufacturing Campaign Reports for items covered in contract CLINS	Electronic copy	<u>Draft</u> : 15 days prior to Regulatory submission. <u>Final</u> : concurrently or 1 business day after submission.
11	Supply Chain Resiliency Plan	Electronic copy	1 months after contract initiation.

C.5. Adjustments to the Reservation Period – Timeline and Cost:

- C.5.1. If the vaccine or therapeutic product sponsor(s) is not consuming the entire reserved capacity (e.g. but not limited to, the product fails in clinical trials, or they don't have the bulk to support continued use of the filling line), the government reserves the option to move that reservation to another government funded product or, with a 90-day written notice to the awardee, release that reserved capacity. If the government changes the product, the government will not have to pay another reservation fee. If the government and awardee agree to release the reservation, the prices associated with the unused reservation will be deobligated from the contract minus a pre-determined early termination fee.
- C.5.2. If the contracted fill and finish manufacturing process requires changes as a result of the approved vaccine or therapeutic product(s), the government and awardee agree to execute a bi-lateral contract modification. If the terms and conditions of the bi-lateral contract modification results in price decreases or increases, the government and awardee will negotiate the required prices changes as applicable.
- C.5.3. The government intends to acquire reservation of vial fill and finish capabilities from the contractor for a period of performance (PoP) IAW the contract delivery schedule. The value of the capacity acquired shall be the sum of the reservation fee and the fill and finish operations. The reservation fee represents a payment for the contractor setting aside the fill finish manufacturing capabilities solely for the government use. The fill and finish operation costs will be paid monthly, less any offsets paid by a third party customer identified by the government. If the government releases the capacity, the fill and finish operation costs shall be paid monthly, less any offsets paid by a third party identified by the contractor. In the event neither the government nor the contractor are able to utilize the capacity during the contract PoP, the scheduled payment will remain unchanged.

The government shall identify third party entities who will be authorized and scheduled to utilize this capacity. The contractor and the third party entity shall separately negotiate a usage fee based on quantity and duration of use. The negotiated price for any fill and finish activity contemplated by this contract and invoiced against the third parties shall be reported to the government monthly and shall be used as the basis to modify the contract to reduce the government's scheduled payment.

C.6. Applicable Document:

C.6.1. Title 42, Public Health; Code of Federal Regulations, Public Health Service, Department of Health and Human Services; Part 73, Select Agents and Toxins. (https://www.ecfr.gov/cgi-bin/text-idx?SID=cdbcfac015041e0bc54c92026504ec82&mc=true&tpl=/ecfrbrowse/Title42/42cfrv1 02.tpl#0)

C.7 Acronym Listing:

Table 2

111010 2			
ACRONYM	DEFINITION		
BARDA Biomedical Advanced Research and Development Authority			
BSL	Biosafety Level		
COVID-19	Coronavirus Disease 2019		
FDA	Federal Drug Administration		
cGMP	Current Good Manufacturing Practices		
HHS	Health and Human Services		
USG	United States government		

Supplies/services will be inspected/accepted at:

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
0001	Destination	Government	Destination	Government
000101	N/A	N/A	N/A	N/A
0002	Destination	Government	Destination	Government
000201	N/A	N/A	N/A	N/A
0003	N/A	N/A	N/A	Government

DELIVERY INFORMATION

CLIN	DELIVERY DATE	QUANTITY	SHIP TO ADDRESS	DODAAC / CAGE
0001	(b) (4)	N/A	BARDA (b) (6) BIOMEDICAL ADVANCED RESEARCH DEVELOPMENT AUTH 200 C STREET, SW WASHINGTON DC 20024 (b) (6) FOB: Destination	(b) (6)
000101	N/A	N/A	N/A	N/A
0002	(b) (4)	N/A	BARDA (b) (6) BIOMEDICAL ADVANCED RESEARCH DEVELOPMENT AUTH 200 C STREET, SW WASHINGTON DC 20024 (b) (6) FOB: Destination	(b) (6)
000201	N/A	N/A	N/A	N/A
0003	(b) (4)	N/A	BARDA (b) (6) BIOMEDICAL ADVANCED RESEARCH DEVELOPMENT AUTH 200 C STREET, SW WASHINGTON DC 20024 (b) (6) FOB: Destination	(b) (6)

ADDITIONAL SHIPPING INFO

SECTION F DELIVERIES OR PERFORMANCE

- **F.1. Supply Chain Resiliency Plan:** The contractor shall develop and submit within 30 calendar days of contract award, a comprehensive Supply Chain Resiliency Program that provides identification and reporting of critical components associated with the secure supply of drug substance, drug product, and work-in-process through to finished goods.
- a) A critical component is defined as any material that is essential to the product or the manufacturing process associated with that product. Included in the definition are consumables and disposables associated with manufacturing. NOT included in the definition are facility and capital equipment.

Consideration of critical components includes the evaluation and potential impact of raw materials, excipients, active ingredients, substances, pieces, parts, software, firmware, labeling, assembly, testing, analytical and environmental componentry, reagents, or utility materials which are used in the manufacturing of a drug, cell banks, seed stocks, devices and key processing components and equipment. A clear example of a critical component is one where a sole supplier is utilized.

The contractor shall identify key equipment suppliers, their locations, local resources, and the associated control processes at the time of award. This document shall address planning and scheduling for active pharmaceutical ingredients, upstream, downstream, component assembly, finished drug product and delivery events as necessary for the delivery of product.

- Communication for these requirements shall be updated as part of an annual review, or as necessary, as part of regular contractual communications.
- b) For upstream and downstream processing, both single-use and re-usable in-place processing equipment, and manufacturing disposables also shall be addressed. For finished goods, the inspection, labeling, packaging, and associated machinery shall be addressed taking into account capacity capabilities.
- c) The focus on the aspects of resiliency shall be on critical components and aspects of complying with the contractual delivery schedule. Delivery methods shall be addressed, inclusive of items that are foreign-sourced, both high and low volume, which would significantly affect throughput and adherence to the contractually agreed deliveries.

The contractor shall articulate in the plan, the methodology for inventory control, production planning, scheduling processes and ordering mechanisms, as part of those agreed deliveries.

- a) Production rates and lead times shall be understood and communicated to the Contracting Officer or the Contracting Officer's Representative as necessary.
- b) Production throughput critical constraints should be well understood by activity and by design, and communicated to contractual personnel. As necessary, communication should focus on identification, exploitation, elevation, and secondary constraints of throughput, as appropriate.

Reports for critical items should include the following information:

- a) Critical Material
- b) Vendor
- c) Supplier, Manufacturing / Distribution Location
- d) Supplier Lead Time
- e) Shelf Life
- f) Transportation / Shipping restrictions

The CO and COR reserve the right to request un-redacted copies of technical documents, during the period of performance, for distribution within the Government. Documents shall be provided within ten (10) days after CO issues the request. The Contractor may arrange for additional time if deemed necessary, and agreed to by the CO.

F.2. Manufacturing Data Requirements: The Contractor shall submit within 30 calendar days of contract award detailed data regarding project materials, sources, and manufacturing sites, including but not limited to: physical locations of sources of raw and processed material by type of material; location and nature of work performed at

manufacturing, processing, and fill/finish sites; and location and nature of non-clinical and clinical studies sites. The Government may provide a table in tabular format for Contractor to be used to submit such data which would include but not be limited to the following:

- Storage/inventory of ancillary materials (vials, needles, syringes, etc.)
- Shipment of ancillary materials (vials, needles, syringes, etc.)
- Disposal of ancillary materials (vials, needles, syringes, etc.)
- Seed development or other starting material manufacturing
- Bulk drug substance and/or adjuvant production
- Fill, finish, and release of product or adjuvant
- Storage/inventory of starting materials, bulk substance, or filled/final product or adjuvant
- Stability information of bulk substance and/or finished product
- Shipment of bulk substance of final product
- Disposal of bulk substance or final product

F.3. Product Development Source Material and Manufacturing Reports and Projections: The Contractor shall submit a detailed spreadsheet regarding critical project materials that are sourced from a location other than the United States, sources, and manufacturing sites, including but not limited to: physical locations of sources of raw and processed material by type of material; location and nature of work performed at manufacturing sites; and location and nature of non-clinical and clinical study sites.

The Contractor will provide manufacturing reports and manufacturing dose tracking projections/actuals utilizing the "COVID-19 Dose Tracking Templates", on any contract/agreement that is manufacturing product:

- Contractor will submit Product Development Source Material Report
 - Within month of contract award
 - o Within 30 days of substantive changes are made to sources and/or materials
 - o and on the 6th month contract anniversary.
- Contractor will update the Dose Tracking Template weekly, during manufacturing campaigns and COVID response, with the first deliverable submission within 15 days of award/modification
- The Government will provide written comments to the Product Development Source Material and Manufacturing Report within 15 business days after the submission
- If corrective action is recommended, Contractor must address all concerns raised by the Government in writing

F.4. Contractor Locations: The contractor shall submit detailed data regarding locations where work will be performed under this contract, including addresses, points of contact, and work performed per location, to include sub-contractors.

Contractor will submit Work Locations Report:

- Within 5 business days of contract award
- Within 30 business days after a substantive location or capabilities change
- Within 2 business days of a substantive change if the work performed supports medical countermeasure development that addresses a threat that has been declared a Public Health Emergency by the HHS Secretary or a Public Health Emergency of International Concern (PHEIC) by the WHO

F.5. Access and General Protection/Security Policy and Procedures: This standard language text is applicable to ALL employees working on critical information related to Operation Warp Speed (OWS), and to those with an area of performance within a Government controlled installation, facility or area. Employees shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative). The performer also shall provide all information required for background checks necessary to access critical information related to OWS, and to meet Government installation access requirements to be accomplished by installation Director of Emergency Services or Security Office. The workforce must comply with all personnel identity verification requirements as directed by the Government and/or

local policy. In addition to the changes otherwise authorized by the changes clause of this agreement, should the security status of OWS change the Government may require changes in performer security matters or processes. In addition to the industry standards for employment background checks, The Contractor must be willing to have key individuals, in exceptionally sensitive positions, identified for additional vetting by the United States Government.

- **F.6. Operational Security (OPSEC):** The performer shall develop an OPSEC Standard Operating Procedure (SOP)/Plan within ninety (90)-calendar-days of project award to be reviewed and approved by the responsible Government OPSEC officer. This plan will be submitted to the COR for coordination of approvals. This SOP/Plan will include identifying the critical information related to this contract, why it needs to be protected, where it is located, who is responsible for it, and how to protect it.
- **F.7. Security Plan:** The contractor shall develop a comprehensive security program that provides overall protection of personnel, information, data, and facilities associated with fulfilling the Government requirement. This plan shall establish security practices and procedures that demonstrate how the contractor will meet and adhere to the security requirements outlined below prior to the commencement of product manufacturing, and shall be delivered to the Government within 30 calendar days of award. The contractor shall also ensure all subcontractors, consultants, researchers, etc. performing work on behalf of this effort, comply with all Government security requirements and prime contractor security plans.
- a) The Government will review in detail and submit comments within ten (10) business days to the Contracting Officer (CO) to be forwarded to the Contractor. The Contractor shall review the Draft Security Plan comments, and, submit a Final Security Plan to the U.S. Government within (10) calendar days after receipt of the comments.
- b) The Security Plan shall include a timeline for compliance of all the required security measures outlined by the Government.
- c) Upon completion of initiating all security measures, the Contractor shall supply to the Contracting Officer a letter certifying compliance to the elements outlined in the Final Security Plan.

At a minimum, the Final Security Plan shall address the following items:

Security Requirements:

1. Facility Security Plan						
Description: As part of the pa	rtner facility's overall security program, the contractor shall submit a written					
security plan with their propo	sal to the Government for review and approval by Government security subject					
matter experts. The performan	nce of work under the contract will be in accordance with the approved security					
plan. The security plan will in	aclude the following processes and procedures at a minimum:					
	organization chart and responsibilities					
Security Administration	written security risk assessment for site					
	 threat levels with identification matrix (High, Medium, or Low) 					
	enhanced security procedures during elevated threats					
	liaison procedures with law enforcement					
	annual employee security education and training program					
	policies and procedures					
Personnel Security	candidate recruitment process					
	 background investigations process 					
	employment suitability policy					
	employee access determination					
	rules of behavior/ conduct					
	termination procedures					
	non-disclosure agreements					
Physical Security Policies	internal/external access control					
and Procedures	protective services					
	identification/badging					

	employee and visitor access controls
	 parking areas and access control
	perimeter fencing/barriers
	 product shipping, receiving and transport security procedures
	facility security lighting
	restricted areas
	• signage
	intrusion detection systems
	alarm monitoring/response
	closed circuit television
	product storage security
	other control measures as identified
Information Security	identification and marking of sensitive information
	access control
	storage of information
	document control procedures
	retention/ destruction requirements
Information	 intrusion detection and prevention systems
Technology/Cyber Security	threat identification
Policies and Procedures	employee training (initial and annual)
	encryption systems
	 identification of sensitive information/media
	 password policy (max days 90)
	 lock screen time out policy (minimum time 20 minutes)
	removable media policy
	laptop policy
	 removal of IT assets for domestic/foreign travel
	access control and determination
	VPN procedures
	WiFi and Bluetooth disabled when not in use
	system document control
	system backup
	system disaster recovery
	incident response
	system audit procedures
	property accountability
2. Site Security Maste	r Plan

2. Site Security Master Plan

Description: The partner facility shall provide a site schematic for security systems which includes: main access points; security cameras; electronic access points; IT Server Room; Product Storage Freezer/Room; and biocontainment laboratories.

3. Site Threat / Vulnerability / Risk Assessment

Description: The partner facility shall provide a written risk assessment for the facility addressing: criminal threat, including crime data; foreign/domestic terrorist threat; industrial espionage; insider threats; natural disasters; and potential loss of critical infrastructure (power/water/natural gas, etc.) This assessment shall include recent data obtained from local law enforcement agencies. The assessment should be updated annually.

4. Physical Security	
Description:	
Closed Circuit Television	a) Layered (internal/external) CCTV coverage with time-lapse video
(CCTV) Monitoring	recording for buildings and areas where critical assets are processed or
	stored.

	b)	CCTV coverage must include entry and exits to critical facilities,
	U)	perimeters, and areas within the facility deemed critical to the execution
		•
	. `	of the contract.
	c)	Video recordings must be maintained for a minimum of 30 days.
	d)	CCTV surveillance system must be on emergency power backup.
	e)	CCTV coverage must include entry and exits to critical facilities,
		perimeters, and areas within the facility deemed critical to the execution
		of the contract.
	f)	Video recordings must be maintained for a minimum of 30 days.
	g)	CCTV surveillance system must be on emergency power backup.
Facility Lighting	a)	Lighting must cover facility perimeter, parking areas, critical
		infrastructure, and entrances and exits to buildings.
	b)	Lighting must have emergency power backup.
	c)	Lighting must be sufficient for the effective operation of the CCTV
		surveillance system during hours of darkness.
Shipping and Receiving	a)	Must have CCTV coverage and an electronic access control system.
	b)	Must have procedures in place to control access and movement of drivers
	· ·	picking up or delivering shipments.
	c)	Must identify drivers picking up Government products by government
	,	issued photo identification.
Access Control	a)	Must have an electronic intrusion detection system with centralized
	/	monitoring.
	b)	Responses to alarms must be immediate and documented in writing.
	c)	Employ an electronic system (i.e., card key) to control access to areas
	()	where assets critical to the contract are located (facilities, laboratories,
		clean rooms, production facilities, warehouses, server rooms, records
		storage, etc.).
	d)	The electronic access control should signal an alarm notification of
	u)	unauthorized attempts to access restricted areas.
	e)	Must have a system that provides a historical log of all key access
		transactions and kept on record for a minimum of 12 months.
	f)	Must have procedures in place to track issuance of access cards to
	1)	employees and the ability to deactivate cards when they are lost or an
		employee leaves the company.
	g)	Response to electronic access control alarms must be immediate and
	g)	documented in writing and kept on record for a minimum of 12 months.
	h)	Should have written procedures to prevent employee piggybacking
	11)	access
	:)	
	i)	to critical infrastructure (generators, air handlers, fuel storage, etc.)
		should be controlled and limited to those with a legitimate need for
	:,	access. Must have a written manual key accountability and inventory process
	j)	Must have a written manual key accountability and inventory process.
	k)	Physical access controls should present a layered approach to critical
Employag/Visitor	2)	assets within the facility. Should issue company photo identification to all ampleyees
Employee/Visitor Identification	a)	Should issue company photo identification to all employees.
Identification	b)	Photo identification should be displayed above the waist anytime the
		employee is on company property.
	c)	Visitors should be sponsored by an employee and must present
	1\	government issued photo identification to enter the property.
	d)	Visitors should be logged in and out of the facility and should be escorted
G : F	D .	by an employee while on the premises at all times.
Security Fencing		ments for security fencing will be determined by the criticality of the
		n, review of the security plan, threat assessment, and onsite security
	assessm	ent.

Protective Security Forces	Requirements for security officers will be determined by the criticality of the
	program, review of the security plan, threat assessment, and onsite security
	assessment.
Protective Security Forces	a) Must have in-service training program.
Operations	b) Must have Use of Force Continuum.
	 Must have communication systems available (i.e., landline on post, cell
	phones, handheld radio, and desktop computer).
	d) Must have Standing Post Orders.
	e) Must wear distinct uniform identifying them as security officers.
5. Security Operation	s
Description:	
Information Sharing	a) Establish formal liaison with law enforcement.
	b) Meet in person at a minimum annually. Document meeting notes and
	keep them on file for a, minimum of 12 months. POC information for LE
	Officer that attended the meeting must be documented.
	c) Implement procedures for receiving and disseminating threat
	information.
Training	a) Conduct new employee security awareness training.
	b) Conduct and maintain records of annual security awareness training.
Security Management	a) Designate a knowledgeable security professional to manage the security
	of the facility.
	b) Ensure subcontractor compliance with all Government security
	requirements.
6. Personnel Security	
Description:	
Records Checks	
	Verification of social security number, date of birth, citizenship, education
	credentials, five-year previous employment history, five-year previous residence
	history, FDA disbarment, sex offender registry, credit check based upon position
	within the company; motor vehicle records check as appropriate; and
7711 170 1	local/national criminal history search.
Hiring and Retention	a) Detailed policies and procedures concerning hiring and retention of
Standards	employees, employee conduct, and off boarding procedures.
	b) Off Boarding procedures should be accomplished within 24 hour of
	employee leaving the company. This includes termination of all network
7 7 6 4 6	access.
7. Information Securi	ty
Description:	A - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -
Physical Document Control	a) Applicable documents shall be identified and marked as procurement
	sensitive, proprietary, or with appropriate government markings.
	b) Sensitive, proprietary, and government documents should be maintained in a localeble filing achieve (dock or other storage daying and not be left
	in a lockable filing cabinet/desk or other storage device and not be left unattended.
	c) Access to sensitive information should be restricted to those with a need to know.
Document Destruction	Documents must be destroyed using approved destruction measures (i.e,
Document Destruction	shredders/approved third party vendors / pulverizing / incinerating).
8. Information Techn	ology & Cybersecurity
	ology & Cybersecurity
Description: Identity Management	a) Physical devices and systems within the organization are inventoried and
identity ivianagement	a) Physical devices and systems within the organization are inventoried and accounted for annually.
	b) Organizational cybersecurity policy is established and communicated.
	c) Asset vulnerabilities are identified and documented.
	c) Asset vulneraumities are identified and documented.

d) Cyber threat intelligence is received from information sharing forums and sources. e) Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. f) Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. g) Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) Access Control a) Limit information system users, processes acting on behalf of users, or devices and authenticate identities before allowing access. c) Limit physical access to information systems, equipment, and server rooms with electronic access controls. d) Limit access to verify access to use of external information systems. Training a) Ensure that personnel are trained and are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Stablish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish an operational incident handling capability for information systems to ensure the availabili			
c) Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. 1 Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. 2 Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) Access Control 2 Limit information system access to authorized users. 3 Identify information system suces, processes acting on behalf of users, or devices and authenticate identities before allowing access. 4 Cares of the control of the co			and
risk. f) Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. g) Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) Access Control a) Limit information system users, processes acting on behalf of users, or devices and authenticate identities before allowing access. c) Limit physical access to information systems, equipment, and server rooms with electronic access controls. d) Limit access to verify access to use of external information systems. Training a) Ensure that personnel are trained and are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic seans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information, analysis, containment, and recovery of epheracianion, detection, analysis, containment, and			Δ
Figure F			
audited for authorized devices, users and processes. g) Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) Access Control a) Limit information system users, processes acting on behalf of users, or devices and authenticate identities before allowing access. c) Limit physical access to information systems, equipment, and server rooms with electronic access controls. d) Limit access to verify access to use of external information systems. Training a) Ensure that personnel are trained and are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Perform periodic scans of the information system components that are physically or logically separated from internal networks. Establish and enforce security configuration settings. Establish and perforce security configuration settings. Establish and perforce security configuration settings. Establish and operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information a) Protect information system me			
multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) Access Control a) Limit information system access to authorized users. b) Identify information system users, processes acting on behalf of users, or devices and authenticate identities before allowing access. c) Limit physical access to information systems, equipment, and server rooms with electronic access controls. d) Limit access to verify access to use of external information systems. a) Ensure that personnel are trained and are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information a) Protection and prevention on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physi			
individuals' security and privacy risks and other organizational risks) Access Control a) Limit information system access to authorized users. b) Identify information system users, processes acting on behalf of users, or devices and authenticate identities before allowing access. c) Limit physical access to information systems, equipment, and server rooms with electronic access controls. d) Limit access tol verify access to use of external information systems. Training a) Ensure that presonnel are trained and are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish and pentanola inclient handling capability for information systems to ensure the availability of critical information resources at all times. backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Establish an operational inclient handling capability for information systems dea dequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability ann			
Access Control a) Limit information system access to authorized users. b) Identify information system users, processes acting on behalf of users, or devices and authenticate identities before allowing access. c) Limit physical access to information systems, equipment, and server rooms with electronic access controls. d) Limit access to verify access to use of external information systems. a) Ensure that personnel are trained and are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital b) Limit a			
b) Identify information system users, processes acting on behalf of users, or devices and authenticate identities before allowing access. c) Limit physical access to information systems, equipment, and server rooms with electronic access controls. d) Limit access to/verify access to use of external information systems. Training a) Ensure that personnel are trained and are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy	A		
devices and authenticate identities before allowing access. c) Limit physical access to information systems, equipment, and server rooms with electronic access controls. d) Limit access to! verify access to use of external information systems. Training a) Ensure that personnel are trained and are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information b) Limit access to information system media, both paper and digital. Limit access to information systems, equipment, and the respective operating environments to authorized undividuals. b) Intrusion detection and preventi	Access Control		0.5
c) Limit physical access to information systems, equipment, and server rooms with electronic access controls. d) Limit access to verify access to use of external information systems. Training a) Ensure that personnel are trained and are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic seans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Establish and enforce security configuration settings. Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems to denote the availability of critical information resources at all times. Distablish an operational incident handling capability for information systems to ensure the availability annually. Media and Information Protection a) Protect information system media, both paper and digital. Limit access to information system media through technology or policy. A limit access to information system sequinpment, and the respective operating environments to authorized indiv			, or
Training a) Ensure that personnel are trained and are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. Limit access to information system sedia through technology or policy. A) Limit access to information system sequipment, and the respective operating environments to authorized univolated users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Protect the physical and support infrastructure for all information		· · · · · · · · · · · · · · · · · · ·	
Training a) Ensure that personnel are trained and are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion prevention and detection technology with immediate ana			
Training associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. Audit and Accountability associated with their activities and of the applicable laws, policies, standards, regulations, or procedures related to information technology systems. a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish and enforce security configuration settings. Incident Response a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems to ensure the availability of critical information, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection D) Intrusion detection and prevention system e			
Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity.	Training		isks
Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection b) Limit access to information system media, both paper and digital. Control the use of removable media through technology or policy. Juint access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention systems employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Employ intrusion prevention and detection technology with immediate analysis	_	associated with their activities and of the applicable laws, policies,	
Audit and Accountability a) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention systems employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity.			y
needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Records must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			
unlawful, unauthorized, or inappropriate system activity. Records must be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis	Audit and Accountability		
be kept for minimum must be kept for 12 months. b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			_
b) Ensure the actions of individual information system users can be uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			sı
uniquely traced to those users. c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. Protection b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			
c) Update malicious code mechanisms when new releases are available. d) Perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed. Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability or information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information b) Limit access to information system media, both paper and digital. Protection b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection b) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis		· · · · · · · · · · · · · · · · · · ·	
Sestablish and enforce security configuration settings.			
Configuration Management a) Establish and enforce security configuration settings. b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			
b) Implement sub networks for publically accessible system components that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. A) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			ed.
that are physically or logically separated from internal networks. Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. A) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis	Configuration Management		
Contingency Planning a) Establish, implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			'
backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis		that are physicany or logically separated from internal networks.	
backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			
ensure the availability of critical information resources at all times. Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis	Contingency Planning		
Incident Response a) Establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			s to
systems that includes adequate preparation, detection, analysis, containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis	I :1 . D		
containment, and recovery of cybersecurity incidents. Exercise this capability annually. Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis	Incident Response		
Capability annually.			
Media and Information Protection a) Protect information system media, both paper and digital. b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			
Protection b) Limit access to information on information systems media to authorized users. c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis	Media and Information	1 ,	
c) Sanitize and destroy media no longer in use. d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			ed
d) Control the use of removable media through technology or policy. Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis		users.	
Physical and Environmental Protection a) Limit access to information systems, equipment, and the respective operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			
Protection operating environments to authorized individuals. b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			
b) Intrusion detection and prevention system employed on IT networks. c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			
c) Protect the physical and support infrastructure for all information systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis	Protection		
systems. d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			
d) Protect information systems against environmental hazards. e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			
e) Escort visitors and monitor visitor activity. Network Protection Employ intrusion prevention and detection technology with immediate analysis			
Network Protection Employ intrusion prevention and detection technology with immediate analysis			
capabilities.	Network Protection		s
		capabilities.	

9. Transportation Sec	urity	
		s must be implemented to protect materials while in transit from theft,
destruction, manipulation, or		s missi of imprementation to protect matterns while in talliant most their
Drivers	a)	Drivers must be vetted in accordance with Government Personnel
Birvers	u)	Security Requirements.
	b)	Drivers must be trained on specific security and emergency procedures.
		Drivers must be equipped with backup communications.
		Driver identity must be 100 percent confirmed before the pick-up of any
	(1)	Government product.
	e)	Drivers must never leave Government products unattended, and two
		drivers may be required for longer transport routes or critical products
		during times of emergency.
	f)	Truck pickup and deliveries must be logged and kept on record for a
		minimum of 12 months.
Transport Routes	a)	Transport routes should be pre-planned and never deviated from except
		when approved or in the event of an emergency.
	b)	Transport routes should be continuously evaluated based upon new
		threats, significant planned events, weather, and other situations that may
		delay or disrupt transport.
Product Security	a)	Government products must be secured with tamper resistant seals during
		transport, and the transport trailer must be locked and sealed.
		 Tamper resistant seals must be verified as "secure" after the
		product is placed in the transport vehicle.
	b)	Government products should be continually monitored by GPS
		technology while in transport, and any deviations from planned routes
		should be investigated and documented.
	c)	Contingency plans should be in place to keep the product secure during
		emergencies such as accidents and transport vehicle breakdowns.
10. Security Reporting		
		notify the Government Security Team within 24 hours of any activity or
		ed security standards or indicates the loss or theft of government products.
	ssociated	with these incidents will be documented in writing for government
review.		
11. Security Audits		
		to formal security audits conducted at the discretion of the government.
Security audits may include b	oth prime	and subcontractor.

CONTRACT ADMINISTRATION

G.1 Government Contract Administration:

In no event shall any understanding or agreement, contract modification, change order, or other matter in deviation from the terms of this contract between the Contractor and a person other than the Contracting Officer be effective or binding upon the Government. All such actions must be formalized by a proper contractual document executed by the Contracting Officer.

Contracting Officer:



Natick, MA 01760-5011

Procurement Specialist:



Bldg 1, General Greene Avenue Natick, MA 01760-5011

In no event shall any understanding or agreement, contract modification, change order, or other matter in deviation from the terms of this contract between the contractor and a person other than the Contracting Officer be effective or binding upon the government. All such actions must be formalized by a proper contractual document executed by the Contracting Officer.

G.2 Government Technical Points of Contact:

Contracting Officers Representative:

b) (6

Branch Chief CDMO Network

Pharmaceutical Countermeasures Infrastructure (PCI)

Biomedical Advanced Research and Development Authority (BARDA)

Office of the Assistant Secretary for Preparedness and Response (ASPR)

Department of Health and Human Services (HHS)



G.3 Contractor's Contract Administration

Technical Point of Contact:

(b) (6

VP Science and Technology Ology Bioservices, Inc, 13200 NW Nano Court Alachua, FL 32615

(b) (6)

(b) (6)

Administrative Point of Contact:

(b) (6

SVP. Government Contracts

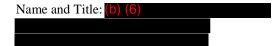
Ology Bioservices, Inc.

8490 Progress Drive, Suite 150, Frederick, MD 21701

(b) (6)

G.4 Contractor's Past Performance Point of Contact (POC):

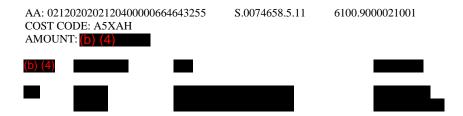
Annual contract past performance evaluations will be performed by the government. The offeror shall identify a Point of Contact (POC) to participate in these on-line evaluations. This individual is required to register in the Contractor Performance Assessment Reporting System (CPARS @ http://www.cpars.csd.disa mil) and respond to the government evaluations in a timely manner. The contractor POC responsible for this action is:



G.5 Notifications of Revisions and Changes:

Notification of revision or changes to names or email addresses will be provided by official correspondence from the PCO/ACO or office of the PCO/ACO in lieu of a contract modification. This does not apply to any such revisions or changes in the event this contract includes a key personnel clause.

ACCOUNTING AND APPROPRIATION DATA



TERMS AND CONDITIONS

SPECIAL CONTRACT REQUIREMENTS

- **H.1.** The government hereby issues this contract action as an Undefinitized Contract Action (UCA) for the reservation of fill and finish manufacturing capacity to secure availability of domestic capacity to perform fill and finish services for government selected COVID-19 vaccine or therapeutics in support of OWS. The UCA award is being executed as a result of the MCM Commercial Solutions Opening (CSO) Solicitation W911QY-20-S-C001 Area of Interest (AOI) Number A001: COVID-19 Fill and Finish Manufacturing Capacity.
- **H.1.1**. This contract shall be definitized NLT 180 days from the date of this award as required by the CONTRACT DEFINITIZATION CLAUSE 252.217-7027. The government intends to obligate (b) (4) upon award of the UCA. The government has developed a definitization schedule that defines the milestone events required to definitize the contract sooner than the required 180 days. The government reserves the right to utilize up to the full 180 day for definitization as required.
- **H.2. Key Personnel:** Any key personnel specified in this contract are considered to be essential to work performance. At least thirty (30) calendar days prior to the contractorvoluntarily diverting any of the specified individuals to other programs or contracts the contractorshall notify the Contracting Officer and shall submit a justification for the diversion or replacement and a request to replace the individual. The request must identify the proposed replacement and provide an explanation of how the replacement's skills, experience, and credentials meet or exceed the requirements of the contract (including, when applicable, Human Subjects Testing requirements). If the employee of the contractoris terminated for cause or separates from the contractorvoluntarily with less than thirty (30) calendar-day notice, the contractorshall provide the maximum notice practicable under the circumstances. The contractorshall not divert, replace, or announce any such change to key personnel without the written consent of the Contracting Officer. The contract will be modified to add or delete key personnel as necessary to reflect the agreement of the parties.

The following individuals are determined to be key personnel:

Name	Title	Role
(b) (6)	Senior Project Manager	Project Manager (PjM). Overall responsibility for the execution of the project. The PjM manages the project team and provides overall project guidance. The PjM regularly communicates on the project's progress and performance with all stakeholders. As the person responsible for the execution of the project, the PjM is the primary Point of Contact, communicator and distributor of information for the project.
(b) (6)	Executive Director, Project Management, Business Operations	Provides high-level program management oversight including CLIN0001 and CLIN0002. Provides financial input and review of product specific proposals. Executive level Program Management governance for any prioritization or escalation with DoD/BARDA and/or Product Sponsor(s)
(b) (6)	Sr Principal Biopharmaceutical Scientist	Principal Investigator. Provides technical and scientific oversight of all scientific aspects of the overarching contract (CLIN0001 and CLIN0002) works closely with the PjM to ensure adherence to program requirements; oversees the technical strategy for CLIN0001 and CLIN0002; reviews and approves study protocols and reports and all other project documents, provides direct oversight of the activities required in performing technology transfer, process scale-up and validation, cGMP manufacturing, product shipping and storage, and stability testing
(b) (6)	Vice President Science and Technology	Provides high-level technical oversight including CLIN0001 and CLIN0002. Provides technical strategy and/or review of product specific proposals. Executive level Technical Management governance for any prioritization or escalation with DoD/BARDA and/or Product Sponsor(s)
(b) (6)	Sr. Manager, Regulatory Affairs	Provide regulatory review of documents and works with subcontractors and product sponsors in providing CMC writing support
(b) (6)	Sr. Director, Quality Assurance	Provides high-level oversight of Quality operations on the project; establishes and maintains quality systems at Ology Bio and at subcontractor sites; oversees maintenance of document archives; oversee Quality Systems at manufacturing and testing site including quality audits and quality agreements; directs oversight of the QA aspects of the project; assures that products, processes, facilities and systems conform to quality standards and government regulations
(b) (6)	Procurement Supervisor	Subcontracting with Sponsors and Subcontractors (JHSS and Bryllan)

H.3. Substitution of Key Personnel: The contractoragrees to assign to the contract those persons whose resumes/CVs were submitted with the proposal who are necessary to fill the requirements of the contract. No substitutions shall be made except in accordance with this guidance. All requests for substitution must provide a detailed explanation of the circumstance necessitating the proposed substitution, a complete resume for the proposed substitute and any other information requested by the contracting officer to approve or disapprove the proposed substitution. All proposed substitutes must have qualifications that are equal to or higher than the qualifications of the person to be replaced. The contracting officer or authorized representative will evaluate such requests and promptly notify the contractor of his approval or disapproval thereof.

The contractor further agrees to include the substance of this language in any subcontract, which may be awarded under this contract.

H.4. Contractor's Organization: The contractor's organization shall be established with authority to effectively accomplish the objectives of the Statement of Work. This organization shall become effective upon award of the contract and its integrity shall be maintained for the duration of the contract effort.

H.5. Disclosure of Information: Performance under this contract may require the contractorto access non-public data and information proprietary to a government agency, another government contractoror of such nature that its dissemination or use other than as specified in the work statement would be adverse to the interests of the government or others. Neither the Contractor, nor contractorpersonnel, shall divulge nor release data nor information developed or obtained under performance of this contract, except authorized by government personnel or upon written approval of the CO in accordance with OWS or other government policies and/or guidance. The contractorshall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as specified in this contract, or any information at all regarding this agency.

The contractorshall comply with all government requirements for protection of non-public information. Unauthorized disclosure of nonpublic information is prohibited by the government's rules. Unauthorized disclosure may result in termination of the contract, replacement of a contractoremployee, or other appropriate redress. Neither the contractornor the Contractor's employees shall disclose or cause to be disseminated, any information concerning the operations of the activity, which could result in, or increase the likelihood of, the possibility of a breach of the activity's security or interrupt the continuity of its operations.

No information related to data obtained under this contract shall be released or publicized without the prior written consent of the COR, whose approval shall not be unreasonably withheld, conditioned, or delayed, provided that no such consent is required to comply with any law, rule, regulation, court ruling or similar order; for submission to any government entity' for submission to any securities exchange on which the Contractor's (or its parent corporation's) securities may be listed for trading; or to third parties relating to securing, seeking, establishing or maintaining regulatory or other legal approvals or compliance, financing and capital raising activities, or mergers, acquisitions, or other business transactions.

- **H.6. Publication and Publicity:** The contractor shall not release any reports, manuscripts, press releases, or abstracts about the work being performed under this contract without written notice in advance to the government.
- (a) Unless otherwise specified in this contract, the contractor may publish the results of its work under this contract. The contractor shall promptly send a copy of each submission to the COR for security review prior to submission. The contractor shall also inform the COR when the abstract article or other publication is published, and furnish a copy of it as finally published.
- (b) Unless authorized in writing by the CO, the contractor shall not display government logos including Operating Division or Staff Division logos on any publications.
- (c) The contractor shall not reference the products(s) or services(s) awarded under this contract in commercial advertising, as defined in FAR 31.205-1, in any manner which states or implies government approval or endorsement of the product(s) or service(s) provided.
- (d) The contractor shall include this language, including this section (d) in all subcontracts where the subcontractor may propose publishing the results of its work under the subcontract. The contractor shall acknowledge the support of the government whenever publicizing the work under this contract in any media by including an acknowledgement substantially as follows:

"This project has been funded in whole or in part by the U.S. government under Contract No. "W911QY-20-C-0101". The US government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notation thereon.

H.7. Confidentiality of Information:

- a. Confidential information, as used in this article, means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.
- b. The Contracting Officer and the contractormay, by mutual consent, identify elsewhere in this contract specific information and/or categories of information which the government will furnish to the contractoror that the contractoris expected to generate which is confidential. Similarly, the Contracting Officer and the contractormay, by

mutual consent, identify such confidential information from time to time during the performance of the contract. Failure to agree will be settled pursuant to the "Disputes" clause.

- c. If it is established elsewhere in this contract that information to be utilized under this contract, or a portion thereof, is subject to the Privacy Act, the contractorwill follow the rules and procedures of disclosure set forth in the Privacy Act of 1974, 5 U.S.C. 552a, and implementing regulations and policies, with respect to systems of records determined to be subject to the Privacy Act.
- d. Confidential information, as defined in paragraph (a) of this article, shall not be disclosed without the prior written consent of the individual, institution, or organization.
- e. Whenever the contractoris uncertain with regard to the proper handling of material under the contract, or if the material in question is subject to the Privacy Act or is confidential information subject to the provisions of this article, the contractorshall obtain a written determination from the Contracting Officer prior to any release, disclosure, dissemination, or publication.
- f. Contracting Officer Determinations will reflect the result of internal coordination with appropriate program and legal officials.
- g. The provisions of paragraph (d) of this article shall not apply to conflicting or overlapping provisions in other Federal, State or local laws.

All above requirements MUST be passed to all Sub-contractors.

H.8. Organizational Conflicts of Interest: Performance under this contract may create an actual or potential organizational conflict of interest such as are contemplated by FAR Part 9.505-General Rules. The contractorshall not engage in any other contractual or other activities which could create an organizational conflict of interest (OCI). This provision shall apply to the prime contractorand all sub-Contractors. This provision shall have effect throughout the period of performance of this contract, any extensions thereto by change order or supplemental agreement, and for two (2) years thereafter. The government may pursue such remedies as may be permitted by law or this contract, upon determination that an OCI has occurred.

The work performed under this contract may create a significant potential for certain conflicts of interest, as set forth in FAR Parts 9.505-1, 9.505-2, 9.505-3, and 9.505-4. It is the intention of the parties hereto to prevent both the potential for bias in connection with the Contractor's performance of this contract, as well as the creation of any unfair competitive advantage as a result of knowledge gained through access to any non-public data or third party proprietary information.

The contractorshall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI. Furthermore, the contractorshall promptly submit a plan to the Contracting Officer to either avoid or mitigate any such OCI. The Contracting Officer will have sole discretion in accepting the Contractor's mitigation plan. In the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, other remedies may be taken to prohibit the contractorfrom participating in contract requirements related to OCI.

Whenever performance of this contract provides access to another Contractor's proprietary information, the contractorshall enter into a written agreement with the other entities involved, as appropriate, in order to protect such proprietary information from unauthorized use or disclosure for as long as it remains proprietary; and refrain from using such proprietary information other than as agreed to, for example to provide assistance during technical evaluation of other Contractors' offers or products under this contract. An executed copy of all proprietary information agreements by individual personnel or on a corporate basis shall be furnished to the CO within fifteen (15) calendar days of execution.

H.9. Institutional Responsibility Regarding Investigator Conflicts of Interest: The Institution (includes any Contractor, public or private, excluding a Federal agency) shall comply with the requirements of 45 CFR Part 94,

Responsible Prospective Contractors, which promotes objectivity in research by establishing standards to ensure that Investigators (defined as the project director or principal Investigator and any other person, regardless of title or position, who is responsible for the design, conduct, or reporting of research funded under government contracts, or proposed for such funding, which may include, for example, collaborators or consultants) will not be biased by any Investigator financial conflicts of interest. 45 CFR Part 94 is available at the following Web site: http://www.ecfr.gov/cgi-

bin/textidx?c=ecfr&SID=0af84ca649a74846f102aaf664da1623&rgn=div5&view=text&node=45:1.0.1.1.51&idno=

As required by 45 CFR Part 94, the Institution shall, at a minimum:

- a. Maintain an up-to-date, written, enforceable policy on financial conflicts of interest that complies with 45 CFR Part 94, inform each Investigator of the policy, the Investigator's reporting responsibilities regarding disclosure of significant financial interests, and the applicable regulation, and make such policy available via a publicly accessible Web site, or if none currently exist, available to any requestor within five business days of a request. A significant financial interest means a financial interest consisting of one or more of the following interests of the Investigator (and those of the Investigator's spouse and dependent children) that reasonably appears to be related to the Investigator's institutional responsibilities:
- 1. With regard to any publicly traded entity, a significant financial interest exists if the value of any remuneration received from the entity in the twelve months preceding the disclosure and the value of any equity interest in the entity as of the date of disclosure, when aggregated, exceeds \$5,000. Included are payments and equity interests;
- 2. With regard to any non-publicly traded entity, a significant financial interest exists if the value of any remuneration received from the entity in the twelve months preceding the disclosure, when aggregated, exceeds \$5,000, or when the Investigator (or the Investigator's spouse or dependent children) holds any equity interest; or
- 3. Intellectual property rights and interests, upon receipt of income related to such rights and interest.

Significant financial interests do not include the following:

- 1. Income from seminars, lectures, or teaching, and service on advisory or review panels for government agencies, Institutions of higher education, academic teaching hospitals, medical centers, or research institutes with an Institution of higher learning; and
- 2. Income from investment vehicles, such as mutual funds and retirement accounts, as long as the Investigator does not directly control the investment decisions made in these vehicles.
- b. Require each Investigator to complete training regarding the Institution's financial conflicts of interest policy prior to engaging in research related to any government funded contract and at least every four years. The Institution must take reasonable steps [see Part 94.4(c)] to ensure that investigators working as collaborators, consultants or subcontractors comply with the regulations.
- c. Designate an official(s) to solicit and review disclosures of significant financial interests from each Investigator who is planning to participate in, or is participating in, the government funded research.
- d. Require that each Investigator who is planning to participate in the government funded research disclose to the Institution's designated official(s) the Investigator's significant financial interest (and those of the Investigator's spouse and dependent children) no later than the date of submission of the Institution's proposal for government funded research. Require that each Investigator who is participating in the government funded research to submit an updated disclosure of significant financial interests at least annually, in accordance with the specific time period prescribed by the Institution during the period of the award as well as within thirty days of discovering or acquiring a new significant financial interest.

- e. Provide guidelines consistent with the regulations for the designated official(s) to determine whether an Investigator's significant financial interest is related to government funded research and, if so related, whether the significant financial interest is a financial conflict of interest. An Investigator's significant financial interest is related to government funded research when the Institution, thorough its designated official(s), reasonably determines that the significant financial interest: Could be affected by the government funded research; or is in an entity whose financial interest could be affected by the research. A financial conflict of interest exists when the Institution, through its designated official(s), reasonably determines that the significant financial interest could directly and significantly affect the design, conduct, or reporting of the government funded research.
- f. Take such actions as necessary to manage financial conflicts of interest, including any financial conflicts of a subcontractor Investigator. Management of an identified financial conflict of interest requires development and implementation of a management plan and, if necessary, a retrospective review and mitigation report pursuant to Part 94.5(a).
- g. Provide initial and ongoing FCOI reports to the Contracting Officer pursuant to Part 94.5(b).
- h. Maintain records relating to all Investigator disclosures of financial interests and the Institution's review of, and response to, such disclosures, and all actions under the Institution's policy or retrospective review, if applicable, for at least 3 years from the date of final payment or, where applicable, for the other time periods specified in 48 CFR Part 4, subpart 4.7, Contract Records Retention.
- i. Establish adequate enforcement mechanisms and provide for employee sanctions or other administrative actions to ensure Investigator compliance as appropriate.
- j. Complete the certification in Section K Representations, Certifications, and Other Statements of Contractors titled "Certification of Institutional Policy on Financial Conflicts of Interest".

If the failure of an Institution to comply with an Institution's financial conflicts of interest policy or a financial conflict of interest management plan appears to have biased the design, conduct, or reporting of the government funded research, the Institution must promptly notify the Contracting Officer of the corrective action taken or to be taken. The Contracting Officer will consider the situation and, as necessary, take appropriate action or refer the matter to the Institution for further action, which may include directions to the Institution on how to maintain appropriate objectivity in the government funded research project.

The Contracting Officer and/or government may inquire at any time before, during, or after award into any Investigator disclosure of financial interests, and the Institution's review of, and response to, such disclosure, regardless of whether the disclosure resulted in the Institution's determination of a financial conflict of interests. The Contracting Officer may require submission of the records or review them on site. On the basis of this review of records or other information that may be available, the Contracting Officer may decide that a particular financial conflict of interest will bias the objectivity of the government funded research to such an extent that further corrective action is needed or that the Institution has not managed the financial conflict of interest in accordance with Part 94.6(b). The issuance of a Stop Work Order by the Contracting Officer may be necessary until the matter is resolved.

If the Contracting Officer determines that government funded clinical research, whose purpose is to evaluate the safety or effectiveness of a drug, medical device, or treatment, has been designed, conducted, or reported by an Investigator with a financial conflict of interest that was not managed or reported by the Institution, the Institution shall require the Investigator involved to disclose the financial conflict of interest in each public presentation of the results of the research and to request an addendum to previously published presentations.

H.10. Cancellation Fee Terms and Conditions: The government and the contractor agree that the following cancellation fee shall be applied to the CLIN 0002:

- a. Should the government cancel or postpone all or part of any purchase less than thirty (30) calendar days prior to the scheduled fill date, the government shall pay to the contractor a non-refundable and non-creditable fee equivalent to (b) of the purchase price of the entire fill.
- b. Should the government cancel or postpone all or part of any purchase more than thirty (30) calendar days and less than sixty (60) calendar days prior to the scheduled fill date, the government shall pay to the contractor a non-refundable and non-creditable fee equivalent to (b) of the purchase price of the entire fill.
- c. Should the government cancel or postpone all or part of any purchase more than sixty (60) calendar days and less than ninety (90) calendar days prior to the scheduled fill date, the government shall pay to the contractor a non-refundable and non-creditable fee equivalent to (b) of the purchase price of the entire fill.
- d. Should the government cancel or postpone all or part of any purchase more than (b) (4) prior to the scheduled fill date, no cancellation or postponement fee will be imposed.

CLIN Cancellation	Time period	(b) fee if cancelled (b) (4)	(b) fee if cancelled between (b) (4)	(b) fee if cancelled between (b) (4)	(b) fee if cancelled between (b)
	01-31 October 2020	9/1/2020	N/A	N/A	N/A
	01-30 November 2020	10/1/2020	9/1/2020	N/A	N/A
	01-31- December 2020	11/1/2020	10/1/2020	9/1/2020	By end of Aug 2020
CLIN 0002	01-31 January 2021	12/1/2020	11/1/2020	10/1/2020	by end of Sept 2020
C2111 0002	01-28 February 2021	1/1/2021	12/1/2020	11/1/2020	by end of Oct 2020
	01-30 April 2021	3/1/2021	2/1/2021	1/1/2021	by end of Dec 2020
	01-31 May 2021	4/1/2021	3/1/2021	2/1/2021	by end of Jan 2021
	01-30 June 2021	5/1/2021	4/1/2021	3/1/2021	by end of Feb 2021
	01-31 July 2021	6/1/2021	5/1/2021	4/1/2021	by end of Mar 2021

H.11. All special requirements list in Section H (H1-H9) shall be included in any subcontract awarded by the contractor. Additionally all contract clauses must flow down to any and all subcontracts award by the contractor.

CLAUSES INCORPORATED BY REFERENCE

52.204-7	System for Award Management	OCT 2018
52.204-13	System for Award Management Maintenance	OCT 2018
52.204-21	Basic Safeguarding of Covered Contractor Information	JUN 2016
	Systems	
52.204-24	Representation Regarding Certain Telecommunications and	DEC 2019
	Video Surveillance Services or Equipment.	
52.212-3 Alt I	Offeror Representations and CertificationsCommercial	OCT 2014
	Items (JUN 2020) Alternate I	

52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
252.203-7000	Requirements Relating to Compensation of Former DoD	SEP 2011
	Officials	
252.203-7003	Agency Office of the Inspector General	AUG 2019
252.204-7012	Safeguarding Covered Defense Information and Cyber	DEC 2019
	Incident Reporting	
252.211-7003	Item Unique Identification and Valuation	MAR 2016
252.232-7003	Electronic Submission of Payment Requests and Receiving	DEC 2018
	Reports	
252.232-7010	Levies on Contract Payments	DEC 2006
252.244-7000	Subcontracts for Commercial Items	JUN 2013

CLAUSES INCORPORATED BY FULL TEXT

52.204-14 SERVICE CONTRACT REPORTING REQUIREMENTS (OCT 2016)

- (a) Definition. First-tier subcontract means a subcontract awarded directly by the Contractor for the purpose of acquiring supplies or services (including construction) for performance of a prime contract. It does not include the Contractor's supplier agreements with vendors, such as long-term arrangements for materials or supplies that benefit multiple contracts and/or the costs of which are normally applied to a Contractor's general and administrative expenses or indirect costs.
- (b) The Contractor shall report, in accordance with paragraphs (c) and (d) of this clause, annually by October 31, for services performed under this contract during the preceding Government fiscal year (October 1-September 30).
- (c) The Contractor shall report the following information:
- (1) Contract number and, as applicable, order number.
- (2) The total dollar amount invoiced for services performed during the previous Government fiscal year under the contract.
- (3) The number of Contractor direct labor hours expended on the services performed during the previous Government fiscal year.
- (4) Data reported by subcontractors under paragraph (f) of this clause.
- (d) The information required in paragraph (c) of this clause shall be submitted via the internet at www.sam.gov. (See SAM User Guide). If the Contractor fails to submit the report in a timely manner, the contracting officer will exercise appropriate contractual remedies. In addition, the Contracting Officer will make the Contractor's failure to comply with the reporting requirements a part of the Contractor's performance information under FAR subpart 42.15.
- (e) Agencies will review Contractor reported information for reasonableness and consistency with available contract information. In the event the agency believes that revisions to the Contractor reported information are warranted, the agency will notify the Contractor no later than November 15. By November 30, the Contractor shall revise the report, or document its rationale for the agency.
- (f)(1) The Contractor shall require each first-tier subcontractor providing services under this contract, with subcontract(s) each valued at or above the thresholds set forth in 4.1703(a)(2), to provide the following detailed information to the Contractor in sufficient time to submit the report:

- (i) Subcontract number (including subcontractor name and unique entity identifier); and
- (ii) The number of first-tier subcontractor direct-labor hours expended on the services performed during the previous Government fiscal year.
- (2) The Contractor shall advise the subcontractor that the information will be made available to the public as required by section 743 of Division C of the Consolidated Appropriations Act, 2010.

(End of clause)

52.212-4 CONTRACT TERMS AND CONDITIONS-- COMMERCIAL ITEMS (OCT 2018)

- (a) Inspection/Acceptance. The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the Government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post-acceptance rights (1) within a reasonable time after the defect was discovered or should have been discovered; and (2) before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.
- (b) Assignment. The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C. 3727). However, when a third party makes payment (e.g., use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.
- (c) Changes. Changes in the terms and conditions of this contract may be made only by written agreement of the parties.
- (d) Disputes. This contract is subject to 41 U.S.C. chapter 71, Contract Disputes", as amended (41 U.S.C. 601-613). Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.
- (e) Definitions. The clause at FAR 52.202-1, Definitions, is incorporated herein by reference.
- (f) Excusable delays. The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement or any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.
- (g) Invoice.
- (1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include--

- (i) Name and address of the Contractor;
- (ii) Invoice date and number;
- (iii) Contract number, line item number and, if applicable, the order number;
- (iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;
- (v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;
- (vi) Terms of any discount for prompt payment offered;
- (vii) Name and address of official to whom payment is to be sent;
- (viii) Name, title, and phone number of person to notify in event of defective invoice; and
- (ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.
- (x) Electronic funds transfer (EFT) banking information.
- (A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.
- (B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer—System for Award Management, or 52.232-34, Payment by Electronic Funds Transfer-Other Than System for Award Management), or applicable agency procedures.
- (C) EFT banking information is not required if the Government waived the requirement to pay by EFT.
- (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 regulations at 5 CFR part 1315.
- (h) Patent indemnity. The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.
- (i) Payment.--
- (1) Items accepted. Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.
- (2) Prompt payment. The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.
- (3) Electronic Funds Transfer (EFT). If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.
- (4) Discount. In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date which appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

- (5) Overpayments. If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall--
- (i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the--
- (A) Circumstances of the overpayment (e.g., duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);
- (B) Affected contract number and delivery order number, if applicable;
- (C) Affected line item or subline item, if applicable; and
- (D) Contractor point of contact.
- (ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.
- (6) Interest.
- (i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C.
- 7109, which is applicable to the period in which the amount becomes due, as provided in (i)(6)(v) of this clause, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.
- (ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.
- (iii) Final decisions. The Contracting Officer will issue a final decision as required by 33.211 if-
- (A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt within 30 days;
- (B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or
- (C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see 32.607-2).
- (iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.
- (v) Amounts shall be due at the earliest of the following dates:
- (A) The date fixed under this contract.
- (B) The date of the first written demand for payment, including any demand for payment resulting from a default termination.
- (vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on--
- (A) The date on which the designated office receives payment from the Contractor;

- (B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or
- (C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.
- (vii) The interest charge made under this clause may be reduced under the procedures prescribed in 32.608-2 of the Federal Acquisition Regulation in effect on the date of this contract.
- (j) Risk of loss. Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:
- (1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or
- (2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.
- (k) Taxes. The contract price includes all applicable Federal, State, and local taxes and duties.
- (1) Termination for the Government's convenience. The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.
- (m) Termination for cause. The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.
- (n) Title. Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.
- (o) Warranty. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.
- (p) Limitation of liability. Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.
- (q) Other compliances. The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.
- (r) Compliance with laws unique to Government contracts. The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 41 U.S.C. 4712 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. chapter 21 relating to procurement integrity.

- (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, Disputes, Payments, Invoice, Other Compliances, Compliance with Laws Unique to Government Contracts, and Unauthorized Obligations paragraphs of this clause; (3) the clause at 52.212-5; (4) addenda to this solicitation or contract, including any license agreements for computer software; (5) solicitation provisions if this is a solicitation; (6) other paragraphs of this clause; (7) the Standard Form 1449; (8) other documents, exhibits, and attachments; and (9) the specification.
- (t) Reserved.
- (u) Unauthorized Obligations.
- (1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any 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 (31 U.S.C. 1341), the following shall govern:
- (i) Any such 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 EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an ``I agree" click box or other comparable mechanism (e.g., ``click-wrap" or ``browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.
- (iii) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.
- (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.
- (v) Incorporation by reference. The Contractor's representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of Clause)

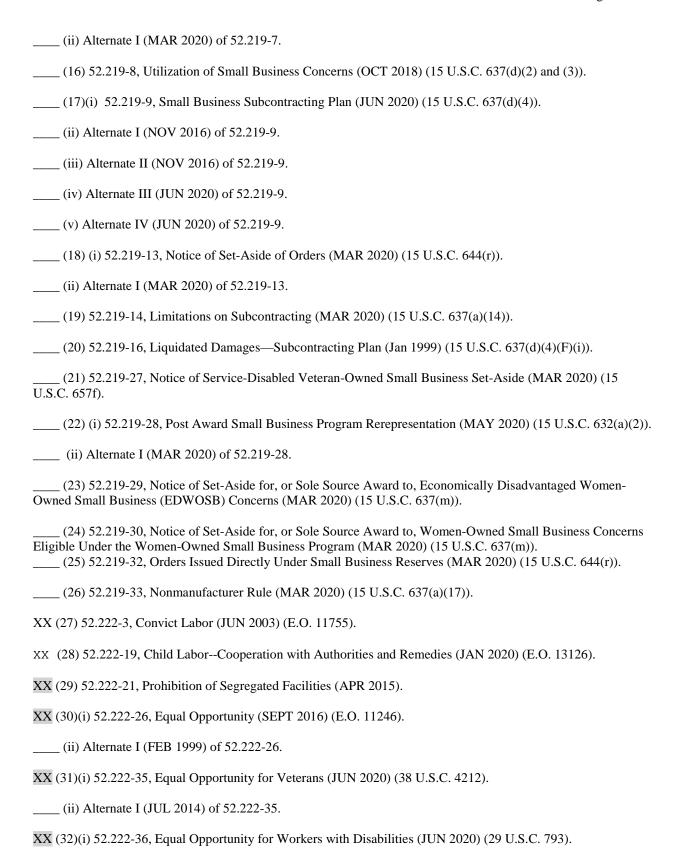
52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (JUL 2020)

- (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 items:
- (1) 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)).
- (2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).
- (3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (AUG 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015). (5) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553). (6) 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 items: (Contracting Officer check as appropriate.) XX (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (JUN 2020), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402). XX (2) 52.203-13, Contractor Code of Business Ethics and Conduct (JUN 2020) (41 U.S.C. 3509). (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.) XX (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] XX (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). XX (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (JUN 2020) (31 U.S.C. 6101 note). XX (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (OCT 2018) (41 U.S.C. 2313). ____ (10) [Reserved] _____(11)(i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (MAR 2020) (15 U.S.C. 657a). ____ (ii) Alternate I (MAR 2020) of 52.219-3. (12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (MAR 2020) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a). (ii) Alternate I (MAR 2020) of 52.219-4. ____ (13) [Reserved] XX (14)(i) 52.219-6, Notice of Total Small Business Set-Aside (MAR 2020) (15 U.S.C. 644).

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

(ii) Alternate I (MAR 2020) of 52.219-6.



(ii) Alternate I (JUL 2014) of 52.222-36.
XX (33) 52.222-37, Employment Reports on Veterans (JUN 2020) (38 U.S.C. 4212).
XX (34) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).
XX (35)(i) 52.222-50, Combating Trafficking in Persons (JAN 2019) (22 U.S.C. chapter 78 and E.O. 13627).
(ii) Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).
XX (36) 52.222-54, Employment Eligibility Verification (OCT 2015). (E. O. 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.)
(37)(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.)
(38) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (JUN 2016) (E.O. 13693).
(39) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (JUN 2016) (E.O. 13693).
(40) (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.
(41)(i) 52.223-14, Acquisition of EPEAT® Registered Televisions (JUN 2014) (E.O.s 13423 and 13514).
(ii) Alternate I (JUN 2014) of 52.223-14.
(42) 52.223-15, Energy Efficiency in Energy-Consuming Products (MAY 2020) (42 U.S.C. 8259b).
(43)(i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (OCT 2015) (E.O.s 13423 and 13514).
(ii) Alternate I (JUN 2014) of 52.223-16.
XX (44) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (JUN 2020) (E.O. 13513).
(45) 52.223-20, Aerosols (JUN 2016) (E.O. 13693).
(46) 52.223-21, Foams (JUN 2016) (E.O. 13693).
(47)(i) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).
(ii) Alternate I (JAN 2017) of 52.224-3.

(48) 52.225-1, Buy AmericanSupplies (MAY 2014) (41 U.S.C. chapter 83).
(49) (i) 52.225-3, Buy AmericanFree Trade AgreementsIsraeli Trade Act (MAY 2014) (41 U.S.C. chapte 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 (MAY 2014) of 52.225-3.
(iii) Alternate II (MAY 2014) of 52.225-3.
(iv) Alternate III (MAY 2014) of 52.225-3.
XX (50) 52.225-5, Trade Agreements (OCT 2019) 19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).
XX (51) 52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
(52) 52.225-26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
(53) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (NOV 2007) (42 U.S.C. 5150
(54) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (NOV 2007) (42 U.S.C. 5150).
(55) 52.229-12, Tax on Certain Foreign Procurements (JUN 2020).
XX (56) 52.232-29, Terms for Financing of Purchases of Commercial Items (FEB 2002) (41 U.S.C. 4505, 10 U.S.C 2307(f)).
(57) 52.232-30, Installment Payments for Commercial Items (JAN 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f))
XX (58) 52.232-33, Payment by Electronic Funds Transfer—System for Award Management (OCT 2018) (31 U.S.C. 3332).
(59) 52.232-34, Payment by Electronic Funds Transfer—Other than System for Award Management (JUL 2013) (31 U.S.C. 3332).
XX (60) 52.232-36, Payment by Third Party (MAY 2014) (31 U.S.C. 3332).
(61) 52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a).
(62) 52.242-5, Payments to Small Business Subcontractors (JAN 2017)(15 U.S.C. 637(d)(13)).
(63)(i) 52.247-64, Preference for Privately Owned U.SFlag Commercial Vessels (FEB 2006) (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 (FEB 2006) 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: (Contracting Officer check as appropriate.)

- XX (1) 52.222-41, Service Contract Labor Standards (AUG 2018) (41 U.S.C. chapter 67).
- XX (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).
- (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).
- _____(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).
- _____(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).
- XX(7) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015) (E.O. 13658).
- XX (8) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).
- _____(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, as defined in FAR 2.101, on the date of award of this contract, 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 (JUN 2020) (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 (Jul 2018) (Section 1634 of Pub. L. 115-91).
- (iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (AUG 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).
- (v) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (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 the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
- (vi) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
- (vii) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).
- (viii) 52.222-35, Equal Opportunity for Veterans (JUN 2020) (38 U.S.C. 4212).
- (ix) 52.222-36, Equal Opportunity for Workers with Disabilities (JUN 2020) (29 U.S.C. 793).
- (x) 52.222-37, Employment Reports on Veterans (JUN 2020) (38 U.S.C. 4212).
- (xi) 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.
- (xii) 52.222-41, Service Contract Labor Standards (Aug 2018), (41 U.S.C. chapter 67).
- (xiii) _____ (A) 52.222-50, Combating Trafficking in Persons (JAN 2019) (22 U.S.C. chapter 78 and E.O. 13627).
- (B) Alternate I (March 2, 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627). (xiv) 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.)
- (xv) 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)
- (xvi) 52.222-54, Employment Eligibility Verification (Oct 2015) (E. O. 12989).
- (xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015) (E.O. 13658).
- (xviii) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706).
- (xix) (A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
- (B) Alternate I (Jan 2017) of 52.224-3.
- (xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
- (xxi) 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.
- (xxii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (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 items a minimal number of additional clauses necessary to satisfy its contractual obligations.
(End of clause)
52.216-23 EXECUTION AND COMMENCEMENT OF WORK (APR 1984)
The Contractor shall indicate acceptance of this letter contract by signing one copy of the contract and returning it to the Contracting Officer not later than 14 August 2020. Upon acceptance by both parties, the Contractor shall proceed with performance of the work, including purchase of necessary materials.
(End of clause)
52.246-15 CERTIFICATE OF CONFORMANCE (APR 1984)
(a) When authorized in writing by the cognizant Contract Administration Office (CAO), the Contractor shall ship with a Certificate of Conformance any supplies for which the contract would otherwise require inspection at source. In no case shall the Government's right to inspect supplies under the inspection provisions of this contract be prejudiced. Shipments of such supplies will not be made under this contract until use of the Certificate of Conformance has been authorized in writing by the CAO, or inspection and acceptance have occurred.
(b) The Contractor's signed certificate shall be attached to or included on the top copy of the inspection or receiving report distributed to the payment office or attached to the CAO copy when contract administration (Block 10 of the DD Form 250) is performed by the Defense Contract Administration Services. In addition, a copy of the signed certificate shall also be attached to or entered on copies of the inspection or receiving report accompanying the shipment.
(c) The Government has the right to reject defective supplies or services within a reasonable time after delivery by written notification to the Contractor. The Contractor shall in such event promptly replace, correct, or repair the rejected supplies or services at the Contractor's expense.
(d) The certificate shall read as follows:
"I certify that on [insert date], the [insert Contractor's name] furnished the supplies or services called for by Contract No via [Carrier] on [identify the bill of lading or shipping document] in accordance with all applicable requirements. I further certify that the supplies or services are of the quality specified and conform in all respects with the contract requirements, including specifications, drawings, preservation, packaging, packing, marking requirements, and physical item identification (part number), and are in the quantity shown on this or on the attached acceptance document."
Date of Execution:
Signature:
Title:

(End of clause)

52.246-16 RESPONSIBILITY FOR SUPPLIES (APR 1984)

- (a) Title to supplies furnished under this contract shall pass to the Government upon formal acceptance, regardless of when or where the Government takes physical possession, unless the contract specifically provides for earlier passage of title.
- (b) Unless the contract specifically provides otherwise, risk of loss of or damage to supplies shall remain with the Contractor until, and shall pass to the Government upon--
- (1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or
- (2) Acceptance by the Government or delivery of the supplies to the Government at the destination specified in the contract, whichever is later, if transportation is f.o.b. destination.
- (c) Paragraph (b) of this section shall not apply to supplies that so fail to conform to contract requirements as to give a right of rejection. The risk of loss of or damage to such nonconforming supplies remains with the Contractor until cure or acceptance. After cure or acceptance, paragraph (b) of this section shall apply.
- (d) Under paragraph (b) of this section, the Contractor shall not be liable for loss of or damage to supplies caused by the negligence of officers, agents, or employees of the Government acting within the scope of their employment.

(End of clause)

252.217-7027 CONTRACT DEFINITIZATION (DEC 2012)

(a) A Undefinitized Contract Action is contemplated. The Contractor agrees to begin promptly negotiating with the Contracting Officer the terms of a definitive contract that will include (1) all clauses required by the Federal Acquisition Regulation (FAR) on the date of execution of the undefinitized contract action, (2) all clauses required by law on the date of execution of the definitive contract action, and (3) any other mutually agreeable clauses, terms, and conditions. The Contractor agrees to submit firm fixed price proposal and other than certified cost or pricing data supporting its proposal.

(b) The schedule for definitizing this contract is as follows:

Receipt of Rough Order of Magnitude (ROM): 3 July 2020

Receipt of Full (Qualifying) Proposal: 10 August 2020

UCA Issued: 14 August 2020

Beginning of Negotiations: 11 September 2020

Complete Negotiations: 2 November 2020

Definitization of UCA: 18 December 2020

- (c) If agreement on a definitive contract action to supersede this undefinitized contract action is not reached by the target date in paragraph (b) of this clause, or within any extension of it granted by the Contracting Officer, the Contracting Officer may, with the approval of the head of the contracting activity, determine a reasonable price or fee in accordance with subpart 15.4 and part 31 of the FAR, subject to Contractor appeal as provided in the Disputes clause. In any event, the Contractor shall proceed with completion of the contract, subject only to the Limitation of Government Liability clause.
- (1) After the Contracting Officer's determination of price or fee, the contract shall be governed by-
- (i) All clauses required by the FAR on the date of execution of this undefinitized contract action for either fixed-price or cost-reimbursement contracts, as determined by the Contracting Officer under this paragraph (c);
- (ii) All clauses required by law as of the date of the Contracting Officer's determination; and
- (iii) Any other clauses, terms, and conditions mutually agreed upon.
- (2) To the extent consistent with paragraph (c)(1) of this clause, all clauses, terms, and conditions included in this undefinitized contract action shall continue in effect, except those that by their nature apply only to an undefinitized contract action.
- (d) The definitive contract resulting from this undefinitized contract action will include a negotiated firm fixed price in no event to exceed (b) (4)

(End of clause)

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (DEC 2018)

- (a) Definitions. As used in this clause—
- "Department of Defense Activity Address Code (DoDAAC)" is a six position code that uniquely identifies a unit, activity, or organization.
- "Document type" means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).
- "Local processing office (LPO)" is the office responsible for payment certification when payment certification is done external to the entitlement system.
- "Payment request" and "receiving report" are defined in the clause at 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.
- (b) Electronic invoicing. The WAWF system provides the method to electronically process vendor payment requests and receiving reports, as authorized by Defense Federal Acquisition Regulation Supplement (DFARS) 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.
- (c) WAWF access. To access WAWF, the Contractor shall—
- (1) Have a designated electronic business point of contact in the System for Award Management at https://www.sam.gov; and
- (2) Be registered to use WAWF at https://wawf.eb mil/ following the step-by-step procedures for self-registration available at this web site.

- (d) WAWF training. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the "Web Based Training" link on the WAWF home page at https://wawf.eb.mil/.
- (e) WAWF methods of document submission. Document submissions may be via web entry, Electronic Data Interchange, or File Transfer Protocol.
- (f) WAWF payment instructions. The Contractor shall use the following information when submitting payment requests and receiving reports in WAWF for this contract or task or delivery order:
- (1) Document type. The Contractor shall submit payment requests using the following document type(s):
- (i) For cost-type line items, including labor-hour or time-and-materials, submit a cost voucher.
- (ii) For fixed price line items—
- (A) That require shipment of a deliverable, submit the invoice and receiving report specified by the Contracting Officer.

Receiving Report (DD 250) Destination Inspection / Destination Acceptance Inspection and Acceptance at place of destination

(B) For services that do not require shipment of a deliverable, submit either the Invoice 2in1, which meets the requirements for the invoice and receiving report, or the applicable invoice and receiving report, as specified by the Contracting Officer.

Invoice as 2-in-1 (FP Services Only – No DD250 Required)

Receiving Report (DD 250) Destination Inspection / Destination Acceptance Inspection and Acceptance at place of destination

- (iii) For customary progress payments based on costs incurred, submit a progress payment request.
- (iv) For performance based payments, submit a performance based payment request.
- (v) For commercial item financing, submit a commercial item financing request.
- (2) Fast Pay requests are only permitted when Federal Acquisition Regulation (FAR) 52.213-1 is included in the contract.

[Note: The Contractor may use a WAWF "combo" document type to create some combinations of invoice and receiving report in one step.]

(3) Document routing. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Field Name in WAWF	Data to be entered in WAWF
Pay Official DoDAAC	(b) (6)
Issue By DoDAAC	(b) (6)
Admin DoDAAC**	(b) (6)
Inspect By DoDAAC	(b) (6)
Ship To Code	(b) (6)
Ship From Code	(b) (6)
Mark For Code	NA
Service Approver (DoDAAC)	(b) (6)
Service Acceptor (DoDAAC)	(b) (6)
Accept at Other DoDAAC	NA
LPO DoDAAC	NA
DCAA Auditor DoDAAC	NA
Other DoDAAC(s)	NA

(*Contracting Officer: Insert applicable DoDAAC information. If multiple ship to/acceptance locations apply, insert "See Schedule" or "Not applicable.")

(**Contracting Officer: If the contract provides for progress payments or performance-based payments, insert the DoDAAC for the contract administration office assigned the functions under FAR 42.302(a)(13).)

- (4) Payment request. The Contractor shall ensure a payment request includes documentation appropriate to the type of payment request in accordance with the payment clause, contract financing clause, or Federal Acquisition Regulation 52.216-7, Allowable Cost and Payment, as applicable.
- (5) Receiving report. The Contractor shall ensure a receiving report meets the requirements of DFARS Appendix F.
- (g) WAWF point of contact.
- (1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

"Not applicable."

 $(2) \ Contact \ the \ WAWF \ help desk \ at \ 866-618-5988, \ if \ assistance \ is \ needed.$

(End of clause)

(b) (4)

- (b) For items(s) identified in paragraph (a) of this clause, the Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "TERMINATION FOR THE CONVENIENCE OF THE GOVERNMENT." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit and estimated termination settlement costs for those item(s).
- (c) Notwithstanding the dates specified in the allotment schedule in paragraph (j) of this clause, the Contractor will notify the Contracting Officer in writing at least ninety days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in paragraph (j) of this clause, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for subsequent period as may be specified in the allotment schedule in paragraph (j) of this clause, or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "TERMINATION FOR THE CONVENIENCE OF THE GOVERNMENT".
- (d) When additional funds are allotted for continued performance of the contract line item(s) identified in paragraph (a) of this clause, the parties will agree as to the period of contract performance which will be covered by the funds. The provisions of paragraph (b) through (d) of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.
- (e) If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract line item(s) identified in paragraph (a) of this clause, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "disputes."
- (f) The Government may at any time prior to termination allot additional funds for the performance of the contract line item(s) identified in paragraph (a) of this clause.
- (g) The termination provisions of this clause do not limit the rights of the Government under the clause entitled "DEFAULT." The provisions of this clause are limited to work and allotment of funds for the contract line item(s) set forth in paragraph (a) of this clause. This clause no longer applies once the contract if fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under paragraphs (d) or (e) of this clause.
- (h) Nothing in this clause affects the right of the Government to this contract pursuant to the clause of this contract entitled "TERMINATION FOR CONVENIENCE OF THE GOVERNMENT."

- (i) Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.
- (j) The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule:

Upon Contract Definitization

(End of clause)

AMENDMENT OF SOLICITA	TION/MODIF	ICATION OF CONTRACT		1 CONTRACT	D CODE	PAGE OF PAGES	;
2 ANTENDATIVE ADDITION TO A TRANSPORT	2 FFFF COM T DAME	A DECUMENTAL PROPERTY OF DEC. NO.	\perp		5 DDOEGEN	1 10	_
2 AMENDMENT/MODIFICATION NO	3 EFFECTIVE DATE 16-Dec-2020	4 REQUISITION/PURCHASE REQ NO SEE SCHEDULE			5 PROJECTN	O (Ifapplicable)	
6 ISSUED BY CODE	W911QY	7 ADMINISTERED BY (Ifother than item 6)		COL	DE W9110	DY .	-
W6QK ACC-APG NATICK DIVISION BLDG 1 GENERAL GREENE AVENUE NATICK MA 01760-5011	wandi	WEGK ACC-APG NATICK CONTRACT NG DIVISION BLDG 1 GENERAL GREENE AVENUE NATICK MA 01760-5011			World	×I	
8. NAME AND ADDRESS OF CONTRACTOR (No Street County S	State and Zin Code)	9A	AMENDMI	ENT OF SOL	ICITATION NO.	_
OLOGY BIOSERVICES, INC NANOTHERAPEUTICS 13200 NW NANO COURT	No., street, County, i	state and Zip Code)	\perp	DATED (SE			_
ALACHUA FL 32615-8726			X 10,	A. MOD. OF 911QY20C01	CONTRACT 01	ORDER NO.	
				B. DATED (SEE ITEM 1	3)	
CODE 3GQS9	FACILITY COL	DE 3GQS9 PPLIES TO AMENDMENTS OF SOLIC	17	-Aug-2020			_
The above numbered solicitation is amended as set forth				xtended.	is not extend	led	\dashv
—		· · · · ·		´ L	is not extend	ied	
Offer must acknowledge receipt of this amendment prior (a) By completing Items 8 and 15, and returning		ified in the solicitation or as amended by one offi it; (b) By acknowledging receipt ofthis amendmen		_	er submitted;		
or (c) By separate letter or telegram which includes a ref	erence to the solicitation	and amendment numbers FAILURE OF YOUR A	CKNOV	VLEDGMENT			
RECEIVED AT THE PLACE DESIGNATED FOR THI REJECTION OF YOUR OFFER If by virtue of this ame					tor		
provided each telegram or letter makes reference to the se	•				iei,		
12. ACCOUNTING AND APPROPRIATION DA See Schedule	TA (If required)						
	M APPLIES ONLY T	O MODIFICATIONS OF CONTRACTS	VORDE	RS.			\neg
IT MODIE	TIES THE CONTRAC	CT/ORDER NO. AS DESCRIBED IN ITE	M 14.				
A. THIS CHANGE ORDER IS ISSUED PURSU. CONTRACT ORDER NO. IN ITEM 10A.	ANT TO: (Specify a	uthority) THE CHANGES SET FORTH	IN ITE	M 14 ARE M	IADE IN TH	E	
B. THE ABOVE NUMBERED CONTRACT/OI office, appropriation date, etc.) SET FORT					as changes in	paying	
C. THIS SUPPLEMENT AL AGREEMENT IS:	ENTERED INTO PU	JRSUANT TO AUTHORITY OF:					
χ D. OTHER (Specify type of modification and a FAR 52.216-25 Contract Definitization	uthority)						
E. IMPORTANT: Contractor is not,	is required to sig	n this document and return 1	copies	to the issuing	g office.		
DESCRIPTION OF AMENDMENT/MODIFIC where feasible.) Modification Control Number: (b) (6 21694) Definitization See Summary of Changes	CATION (Organized	by UCF section headings, including solici	itation/	contract subje	ect matter		
Except as provided herein, all terms and conditions of the do: 15A. NAME AND TITLE OF SIGNER (Type or 1 (b) (6)		9A or 10A, as heretofore changed, remains unchan 16A. NAME AND TITLE OF CO (b) (6) CONTRACT NG OFFICER				r print)	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNE	D 16B <u>UNITED STATES OF AMER</u>	RICA	(0)	16C	DATE SIGNED	_
(b) (6)	December 15, 2020	(b) (6)				-Dec-2020	
(Signature of person authorized to sign)		(Signature of Contracting Off	ficer)		10	200-2020	
EXCEPTION TO SF 30		30-105-04		STA	NDARD FO	RM 30 (Rev. 10-8	(3)

AMENDMENT OF SOLICITA	TION/MODIF	ICATION OF CONTRACT	1 CONTRACT	ID CODE	PAGE OF PAGES
					1 10
2 AMENDMENT/MODIFICATION NO	3 EFFECTIVE DATE	4 REQUISITION/PURCHASE REQ NO		5 PROJECTN	O (Ifapplicable)
PZ0001	16-Dec-2020	SEE SCHEDULE			
6 ISSUED BY CODE W6QK ACC-APG NATICK DIVISION BLDG 1 GENERAL GREENE AVENUE NATICK MA 01760-5011	W911QY	7 ADMINISTERED BY (Ifother than item 6) W6QK ACC-APG NATICK CONTRACT NG DIVISION BLDG 1 GENERAL GREENE AVENUE NATICK MA 01760-5011	coi	DE W9110	QΥ
8. NAME AND ADDRESS OF CONTRACTOR (OLOGY BIOSERVICES, INC NANOTHERAPEUTICS	No., Street, County, S	State and Zip Code)	9A. AMENDMI 9B. DATED (SI		ICIT AT ION NO.
13200 NWNANO COURT ALACHUA FL 32615-8726		-	<u> </u>		
		-	X 10A MOD OF W911QY20C0 10B DATED (
CODE 3GQS9	FACILITY COD	DE 3GQS9	X 17-Aug-2020	•	•
11. 7		PPLIES TO AMENDMENTS OF SOLIC	ITATIONS		
The above numbered solicitation is amended as set forth	in Item 14 The hour and	date specified for receipt of Offer	is extended,	is not extend	led
Offer must acknowledge receipt of this amendment prior (a) By completing Items 8 and 15, and returning or (c) By separate letter or telegram which includes a ref RECEIVED AT THE PLACE DESIGNATED FOR THI REJECTION OF YOUR OFFER If by virtue of this am provided each telegram or letter makes reference to the s	copies of the amendmen erence to the solicitation a RECEIPT OF OFFERS I endment you desire to cha	nt; (b) By acknowledging receipt of this amendmen and amendment numbers FAILURE OF YOUR A PRIOR TO THE HOUR AND DATE SPECIFIED nge an offer already submitted, such change may be	t on each copy of the off CKNOWLEDGMENT MAY RESULT IN e made by telegramor let	го ве	
12. ACCOUNTING AND APPROPRIATION DA	TA (If required)				
See Schedule					
		O MODIFICATIONS OF CONTRACTS T/ORDER NO. AS DESCRIBED IN ITE			
A. THIS CHANGE ORDER IS ISSUED PURSU. CONTRACT ORDER NO. IN ITEM 10A.	ANT TO: (Specify a	uthority) THE CHANGES SET FORTH I	N ITEM 14 ARE M	IADE IN TH	E
B. THE ABOVE NUMBERED CONTRACT/OF office, appropriation date, etc.) SET FORT				as changes in	paying
C. THIS SUPPLEMENT AL AGREEMENT IS:	ENTERED INTO PU	RSUANT TO AUTHORITY OF:			
X D. OTHER (Specify type of modification and a FAR 52.216-25 Contract Definitization	uthority)				
E. IMPORT ANT: Contractor is not,	is required to sig	n this document and return 1	copies to the issuing	g office.	
14. DESCRIPTION OF AMENDMENT/MODIFIC where feasible.) Modification Control Number: 10 16 21694 Definitization See Summary of Changes Except as provided herein, all terms and conditions of the do	CATION (Organized	9A or 10A, as heretofore changed, remains unchan	ged and in fall force and	effect	
15A. NAME AND TITLE OF SIGNER (Type or 1	orint)	16A. NAME AND TITLE OF COM	NTRACTING OFFI	CER (Type o	r print)
		(b) (6)			
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	D 16B. UNITED STATES OF AMER	ICA		DATE SIGNED
(Signature of person authorized to sign)		(Signature of Contracting Off	icer)	16	-Dec-2020

SECTION SF 30 BLOCK 14 CONTINUATION PAGE

SUMMARY OF CHANGES

SECTION SF 30 - BLOCK 14 CONTINUATION PAGE The following have been added by full text: ACTION OBLIGATION AMOUNT: (b) (4) The purpose of this modification is to: 1) Definitize the contract by amending the CLIN values and funding according to the negotiated prices. 2) Decrease the unit and total price of CLIN 0001. 3) Decrease the unit and total price of CLIN 0002. 4) Decrease the total price of the contract. 5) Decrease the funding on CLIN 0001. 6) Increase the funding on CLIN 0002. 7) Remove the definitization clause 252.217-7027 and incremental funding clause 252.232-7007. 8) Update the language in Section H.1. 9) Delete Section H.1.1. Prior to definitization (b) (4) was invoiced against the not-to-exceed price of (b) (4) on CLIN 0001. Through negotiations during the definitization process, the parties agreed to a negotiated price of (b) (4) CLIN 0001. In recognition of the actual amount already invoiced and expended against CLIN 0001, which exceeds the negotiated price by (b) (4) , the USG agrees to a definitized price of (b) (4) for CLIN 0001, and accepts as consideration a reduction by (b) (4) to the negotiated price of CLIN 0002, for a definitized price of SECTION SF 1449 - CONTINUATION SHEET SOLICITATION/CONTRACT FORM The total cost of this contract was decreased by (b) (4) from (b) (4)

SUPPLIES OR SERVICES AND PRICES

	LIN 0001 definitized action has occu The unit price amount l	nas decreased by <mark>(b</mark>) (4)		ı .	
	The cost constraint NT: The total cost of this lin					
SI	UBCLIN 000101 The CLIN description h	nas changed from A	.CRN AA @ <mark>(</mark> b) (4)		
	LIN 0002 definitized action has occurred the unit price amount I The cost constraint NT The total cost of this lin	nas decreased by (b E has been deleted.) (4)			-
	LIN 0003 definitized action has occu	urred in this modific	cation			
SI	UBCLIN 000202 is added	as follows:				
ITEM NO 000202	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE		AMOUNT \$0.00
	ACRN AA @ (b) (4) FFP PURCHASE REQUEST	NUMBER: 00115	33611-0003			
				NET AMT		\$0.00
	ACRN AA CIN: GFEBS001153361	100003				0) (4)
ACCO	UNTING AND APPROPI	RIATION				
Summa	ary for the Payment Office					
A	s a result of this modificati	on, the total funded	l amount for thi	s document was increased	1 by (b) (4)	
SURC	LIN 000101:	•				
SOBO						

AA: 0212020202120400000664643255 S.0074658.5.11 6100.9000021001 A5XAH (CIN GFEBS001153361100001) was decreased by (b) (4)

SUBCLIN 000202:

Funding on SUBCLIN 000202 is initiated as follows:

ACRN: AA

CIN: GFEBS001153361100003

Acctng Data: 0212020202120400000664643255 S.0074658.5.11 6100.9000021001

(b) (4)

Cost Code: A5XAH

INSPECTION AND ACCEPTANCE

The following Acceptance/Inspection Schedule was added for SUBCLIN 000202:

The following have been modified: TERMS AND CONDITIONS

SPECIAL CONTRACT REQUIREMENTS

H.1. The government hereby issues this contract action as a definitized contract action for the reservation of fill and finish manufacturing capacity to secure availability of domestic capacity to perform fill and finish services for government selected COVID-19 vaccine or therapeutics in support of OWS. The award is being executed as a result of the MCM Commercial Solutions Opening (CSO) Solicitation W911QY-20-S-C001 Area of Interest (AOI) Number A001: COVID-19 Fill and Finish Manufacturing Capacity.

H.2. Key Personnel: Any key personnel specified in this contract are considered to be essential to work performance. At least thirty (30) calendar days prior to the contractorvoluntarily diverting any of the specified individuals to other programs or contracts the contractorshall notify the Contracting Officer and shall submit a justification for the diversion or replacement and a request to replace the individual. The request must identify the proposed replacement and provide an explanation of how the replacement's skills, experience, and credentials meet or exceed the requirements of the contract (including, when applicable, Human Subjects Testing requirements). If the employee of the contractoris terminated for cause or separates from the contractorvoluntarily with less than thirty (30) calendarday notice, the contractorshall provide the maximum notice practicable under the circumstances. The contractorshall not divert, replace, or announce any such change to key personnel without the written consent of the Contracting Officer. The contract will be modified to add or delete key personnel as necessary to reflect the agreement of the parties.

The following individuals are determined to be key personnel:

Name	Title	Role
(b) (6)	Senior Project Manager	Project Manager (PjM). Overall responsibility for the execution of the
		project. The PjM manages the project team and provides overall project

		guidance. The PjM regularly communicates on the project's progress and performance with all stakeholders. As the person responsible for the execution of the project, the PjM is the primary Point of Contact, communicator and distributor of information for the project.
(b) (b)	Executive Director, Project Management, Business Operations	Provides high-level program management oversight including CLIN0001 and CLIN0002. Provides financial input and review of product specific proposals. Executive level Program Management governance for any prioritization or escalation with DoD/BARDA and/or Product Sponsor(s)
(b) (6)	Sr Principal Biopharmaceutical Scientist	Principal Investigator. Provides technical and scientific oversight of all scientific aspects of the overarching contract (CLIN0001 and CLIN0002) works closely with the PjM to ensure adherence to program requirements; oversees the technical strategy for CLIN0001 and CLIN0002; reviews and approves study protocols and reports and all other project documents, provides direct oversight of the activities required in performing technology transfer, process scale-up and validation, cGMP manufacturing, product shipping and storage, and stability testing
(b) (6)	Vice President Science and Technology	Provides high-level technical oversight including CLIN0001 and CLIN0002. Provides technical strategy and/or review of product specific proposals. Executive level Technical Management governance for any prioritization or escalation with DoD/BARDA and/or Product Sponsor(s)
(b) (6)	Sr. Manager, Regulatory Affairs	Provide regulatory review of documents and works with subcontractors and product sponsors in providing CMC writing support
(b) (6)	Sr. Director, Quality Assurance	Provides high-level oversight of Quality operations on the project; establishes and maintains quality systems at Ology Bio and at subcontractor sites; oversees maintenance of document archives; oversee Quality Systems at manufacturing and testing site including quality audits and quality agreements; directs oversight of the QA aspects of the project; assures that products, processes, facilities and systems conform to quality standards and government regulations
(b) (6)	Procurement Supervisor	Subcontracting with Sponsors and Subcontractors (JHSS and Bryllan)

H.3. Substitution of Key Personnel: The contractoragrees to assign to the contract those persons whose resumes/CVs were submitted with the proposal who are necessary to fill the requirements of the contract. No substitutions shall be made except in accordance with this guidance. All requests for substitution must provide a detailed explanation of the circumstance necessitating the proposed substitution, a complete resume for the proposed substitute and any other information requested by the contracting officer to approve or disapprove the proposed substitution. All proposed substitutes must have qualifications that are equal to or higher than the qualifications of the person to be replaced. The contracting officer or authorized representative will evaluate such requests and promptly notify the contractor of his approval or disapproval thereof.

The contractor further agrees to include the substance of this language in any subcontract, which may be awarded under this contract.

- **H.4. Contractor's Organization:** The contractor's organization shall be established with authority to effectively accomplish the objectives of the Statement of Work. This organization shall become effective upon award of the contract and its integrity shall be maintained for the duration of the contract effort.
- **H.5. Disclosure of Information:** Performance under this contract may require the contractorto access non-public data and information proprietary to a government agency, another government contractoror of such nature that its dissemination or use other than as specified in the work statement would be adverse to the interests of the government or others. Neither the Contractor, nor contractorpersonnel, shall divulge nor release data nor information developed

or obtained under performance of this contract, except authorized by government personnel or upon written approval of the CO in accordance with OWS or other government policies and/or guidance. The contractorshall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as specified in this contract, or any information at all regarding this agency.

The contractorshall comply with all government requirements for protection of non-public information. Unauthorized disclosure of nonpublic information is prohibited by the government's rules. Unauthorized disclosure may result in termination of the contract, replacement of a contractoremployee, or other appropriate redress. Neither the contractornor the Contractor's employees shall disclose or cause to be disseminated, any information concerning the operations of the activity, which could result in, or increase the likelihood of, the possibility of a breach of the activity's security or interrupt the continuity of its operations.

No information related to data obtained under this contract shall be released or publicized without the prior written consent of the COR, whose approval shall not be unreasonably withheld, conditioned, or delayed, provided that no such consent is required to comply with any law, rule, regulation, court ruling or similar order; for submission to any government entity' for submission to any securities exchange on which the Contractor's (or its parent corporation's) securities may be listed for trading; or to third parties relating to securing, seeking, establishing or maintaining regulatory or other legal approvals or compliance, financing and capital raising activities, or mergers, acquisitions, or other business transactions.

H.6. Publication and Publicity: The contractor shall not release any reports, manuscripts, press releases, or abstracts about the work being performed under this contract without written notice in advance to the government.

- **a.** Unless otherwise specified in this contract, the contractor may publish the results of its work under this contract. The contractor shall promptly send a copy of each submission to the COR for security review prior to submission. The contractor shall also inform the COR when the abstract article or other publication is published, and furnish a copy of it as finally published.
- **b.** Unless authorized in writing by the CO, the contractor shall not display government logos including Operating Division or Staff Division logos on any publications.
- **c.** The contractor shall not reference the products(s) or services(s) awarded under this contract in commercial advertising, as defined in FAR 31.205-1, in any manner which states or implies government approval or endorsement of the product(s) or service(s) provided.
- **d.** The contractor shall include this language, including this section (d) in all subcontracts where the subcontractor may propose publishing the results of its work under the subcontract. The contractor shall acknowledge the support of the government whenever publicizing the work under this contract in any media by including an acknowledgement substantially as follows:

"This project has been funded in whole or in part by the U.S. government under Contract No. "W911QY-20-C-0101". The US government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notation thereon.

H.7. Confidentiality of Information:

- **a.** Confidential information, as used in this article, means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.
- **b.** The Contracting Officer and the contractormay, by mutual consent, identify elsewhere in this contract specific information and/or categories of information which the government will furnish to the contractoror that the contractoris expected to generate which is confidential. Similarly, the Contracting Officer and the contractormay, by mutual consent, identify such confidential information from time to time during the performance of the contract. Failure to agree will be settled pursuant to the "Disputes" clause.
- c. If it is established elsewhere in this contract that information to be utilized under this contract, or a portion thereof, is subject to the Privacy Act, the contractorwill follow the rules and procedures of disclosure set forth in the Privacy Act of 1974, 5 U.S.C. 552a, and implementing regulations and policies, with respect to systems of records determined to be subject to the Privacy Act.

- **d.** Confidential information, as defined in paragraph (a) of this article, shall not be disclosed without the prior written consent of the individual, institution, or organization.
- **e.** Whenever the contractoris uncertain with regard to the proper handling of material under the contract, or if the material in question is subject to the Privacy Act or is confidential information subject to the provisions of this article, the contractorshall obtain a written determination from the Contracting Officer prior to any release, disclosure, dissemination, or publication.
- **f.** Contracting Officer Determinations will reflect the result of internal coordination with appropriate program and legal officials.
- g. The provisions of paragraph (d) of this article shall not apply to conflicting or overlapping provisions in other Federal, State or local laws.

All above requirements MUST be passed to all Sub-contractors.

H.8. Organizational Conflicts of Interest: Performance under this contract may create an actual or potential organizational conflict of interest such as are contemplated by FAR Part 9.505-General Rules. The contractorshall not engage in any other contractual or other activities which could create an organizational conflict of interest (OCI). This provision shall apply to the prime contractorand all sub-Contractors. This provision shall have effect throughout the period of performance of this contract, any extensions thereto by change order or supplemental agreement, and for two (2) years thereafter. The government may pursue such remedies as may be permitted by law or this contract, upon determination that an OCI has occurred.

The work performed under this contract may create a significant potential for certain conflicts of interest, as set forth in FAR Parts 9.505-1, 9.505-2, 9.505-3, and 9.505-4. It is the intention of the parties hereto to prevent both the potential for bias in connection with the Contractor's performance of this contract, as well as the creation of any unfair competitive advantage as a result of knowledge gained through access to any non-public data or third party proprietary information.

The contractorshall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI. Furthermore, the contractorshall promptly submit a plan to the Contracting Officer to either avoid or mitigate any such OCI. The Contracting Officer will have sole discretion in accepting the Contractor's mitigation plan. In the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, other remedies may be taken to prohibit the contractorfrom participating in contract requirements related to OCI.

Whenever performance of this contract provides access to another Contractor's proprietary information, the contractorshall enter into a written agreement with the other entities involved, as appropriate, in order to protect such proprietary information from unauthorized use or disclosure for as long as it remains proprietary; and refrain from using such proprietary information other than as agreed to, for example to provide assistance during technical evaluation of other Contractors' offers or products under this contract. An executed copy of all proprietary information agreements by individual personnel or on a corporate basis shall be furnished to the CO within fifteen (15) calendar days of execution.

H.9. Institutional Responsibility Regarding Investigator Conflicts of Interest: The Institution (includes any Contractor, public or private, excluding a Federal agency) shall comply with the requirements of 45 CFR Part 94, Responsible Prospective Contractors, which promotes objectivity in research by establishing standards to ensure that Investigators (defined as the project director or principal Investigator and any other person, regardless of title or position, who is responsible for the design, conduct, or reporting of research funded under government contracts, or proposed for such funding, which may include, for example, collaborators or consultants) will not be biased by any Investigator financial conflicts of interest. 45 CFR Part 94 is available at the following Web site: http://www.ecfr.gov/cgi-

bin/textidx?c=ecfr&SID=0af84ca649a74846f102aaf664da1623&rgn=div5&view=text&node=45:1.0.1.1.51&idno=

As required by 45 CFR Part 94, the Institution shall, at a minimum:

- **a.** Maintain an up-to-date, written, enforceable policy on financial conflicts of interest that complies with 45 CFR Part 94, inform each Investigator of the policy, the Investigator's reporting responsibilities regarding disclosure of significant financial interests, and the applicable regulation, and make such policy available via a publicly accessible Web site, or if none currently exist, available to any requestor within five business days of a request. A significant financial interest means a financial interest consisting of one or more of the following interests of the Investigator (and those of the Investigator's spouse and dependent children) that reasonably appears to be related to the Investigator's institutional responsibilities:
- 1. With regard to any publicly traded entity, a significant financial interest exists if the value of any remuneration received from the entity in the twelve months preceding the disclosure and the value of any equity interest in the entity as of the date of disclosure, when aggregated, exceeds \$5,000. Included are payments and equity interests;
- 2. With regard to any non-publicly traded entity, a significant financial interest exists if the value of any remuneration received from the entity in the twelve months preceding the disclosure, when aggregated, exceeds \$5,000, or when the Investigator (or the Investigator's spouse or dependent children) holds any equity interest; or
- 3. Intellectual property rights and interests, upon receipt of income related to such rights and interest.

Significant financial interests do not include the following:

- 1. Income from seminars, lectures, or teaching, and service on advisory or review panels for government agencies, Institutions of higher education, academic teaching hospitals, medical centers, or research institutes with an Institution of higher learning; and
- 2. Income from investment vehicles, such as mutual funds and retirement accounts, as long as the Investigator does not directly control the investment decisions made in these vehicles.
- **a.** Require each Investigator to complete training regarding the Institution's financial conflicts of interest policy prior to engaging in research related to any government funded contract and at least every four years. The Institution must take reasonable steps [see Part 94.4(c)] to ensure that investigators working as collaborators, consultants or subcontractors comply with the regulations.
- **b.** Designate an official(s) to solicit and review disclosures of significant financial interests from each Investigator who is planning to participate in, or is participating in, the government funded research.
- c. Require that each Investigator who is planning to participate in the government funded research disclose to the Institution's designated official(s) the Investigator's significant financial interest (and those of the Investigator's spouse and dependent children) no later than the date of submission of the Institution's proposal for government funded research. Require that each Investigator who is participating in the government funded research to submit an updated disclosure of significant financial interests at least annually, in accordance with the specific time period prescribed by the Institution during the period of the award as well as within thirty days of discovering or acquiring a new significant financial interest.
- **d.** Provide guidelines consistent with the regulations for the designated official(s) to determine whether an Investigator's significant financial interest is related to government funded research and, if so related, whether the significant financial interest is a financial conflict of interest. An Investigator's significant financial interest is related to government funded research when the Institution, thorough its designated official(s), reasonably determines that the significant financial interest: Could be affected by the government funded research; or is in an entity whose financial interest could be affected by the research. A financial conflict of interest exists when the Institution, through its designated official(s), reasonably determines that the significant financial interest could directly and significantly affect the design, conduct, or reporting of the government funded research.
- **e.** Take such actions as necessary to manage financial conflicts of interest, including any financial conflicts of a subcontractor Investigator. Management of an identified financial conflict of interest requires development and implementation of a management plan and, if necessary, a retrospective review and mitigation report pursuant to Part 94.5(a).
- **f.** Provide initial and ongoing FCOI reports to the Contracting Officer pursuant to Part 94.5(b).
- **g.** Maintain records relating to all Investigator disclosures of financial interests and the Institution's review of, and response to, such disclosures, and all actions under the Institution's policy or retrospective review, if applicable, for at least 3 years from the date of final payment or, where applicable, for the other time periods specified in 48 CFR Part 4, subpart 4.7, Contract Records Retention.

- **h.** Establish adequate enforcement mechanisms and provide for employee sanctions or other administrative actions to ensure Investigator compliance as appropriate.
- i. Complete the certification in Section K Representations, Certifications, and Other Statements of Contractors titled "Certification of Institutional Policy on Financial Conflicts of Interest".

If the failure of an Institution to comply with an Institution's financial conflicts of interest policy or a financial conflict of interest management plan appears to have biased the design, conduct, or reporting of the government funded research, the Institution must promptly notify the Contracting Officer of the corrective action taken or to be taken. The Contracting Officer will consider the situation and, as necessary, take appropriate action or refer the matter to the Institution for further action, which may include directions to the Institution on how to maintain appropriate objectivity in the government funded research project.

The Contracting Officer and/or government may inquire at any time before, during, or after award into any Investigator disclosure of financial interests, and the Institution's review of, and response to, such disclosure, regardless of whether the disclosure resulted in the Institution's determination of a financial conflict of interests. The Contracting Officer may require submission of the records or review them on site. On the basis of this review of records or other information that may be available, the Contracting Officer may decide that a particular financial conflict of interest will bias the objectivity of the government funded research to such an extent that further corrective action is needed or that the Institution has not managed the financial conflict of interest in accordance with Part 94.6(b). The issuance of a Stop Work Order by the Contracting Officer may be necessary until the matter is resolved.

If the Contracting Officer determines that government funded clinical research, whose purpose is to evaluate the safety or effectiveness of a drug, medical device, or treatment, has been designed, conducted, or reported by an Investigator with a financial conflict of interest that was not managed or reported by the Institution, the Institution shall require the Investigator involved to disclose the financial conflict of interest in each public presentation of the results of the research and to request an addendum to previously published presentations.

H.10. Cancellation Fee Terms and Conditions: The government and the contractor agree that the following cancellation fee shall be applied to the CLIN 0002:

a. Should the government cancel or postpone all or part of any purchase (b) (4) prior to the scheduled fill date, the government shall pay to the contractor a non-refundable and non-creditable fee equivalent to of the purchase price of the entire fill.

b. Should the government cancel or postpone all or part of any purchase (b) (4)

prior to the scheduled fill date, the government shall pay to the contractor a nonrefundable and non-creditable fee equivalent to (b) of the purchase price of the entire fill.

c. Should the government cancel or postpone all or part of any purchase (b) (4)

prior to the scheduled fill date, the government shall pay to the contractor a nonrefundable and non-creditable fee equivalent to (b) of the purchase price of the entire fill.

d. Should the government cancel or postpone all or part of any purchase (b) (4)

will be imposed.

CLIN Cancellation	Time period	(b) fee if cancelled (b) (4)	(b) fee if cancelled between (b) (4)	(b) fee if cancelled between (b) (4)	(b) (4)
	01-31 October 2020	9/1/2020	N/A	N/A	N/A
CLIN 0002	01-30 November 2020	10/1/2020	9/1/2020	N/A	N/A
	01-31- December 2020	11/1/2020	10/1/2020	9/1/2020	By end of Aug 2020
	01-31 January 2021	12/1/2020	11/1/2020	10/1/2020	by end of Sept 2020

01-28 Februa 2021	1/1/2021	12/1/2020	11/1/2020	by end of Oct 2020
01-30 Apri 2021	3/1/2021	2/1/2021	1/1/2021	by end of Dec 2020
01-31 May 2021	4/1/2021	3/1/2021	2/1/2021	by end of Jan 2021
01-30 June 2021	5/1/2021	4/1/2021	3/1/2021	by end of Feb 2021
01-31 July 2021	6/1/2021	5/1/2021	4/1/2021	by end of Mar 2021

H.11. All special requirements list in Section H (H1-H9) shall be included in any subcontract awarded by the contractor. Additionally all contract clauses must flow down to any and all subcontracts award by the contractor.

The following have been deleted:

252.217-7027 Contract Definitization DEC 2012 252.232-7007 Limitation Of Government's Obligation APR 2014

(End of Summary of Changes)