

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED TOP SECRET b. LEVEL OF SAFEGUARD REQUIRED NONE																																																																																					
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>				3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>																																																																																					
☒	a. PRIME CONTRACT NUMBER D16PC00069			☒	a. ORIGINAL <i>(Complete date in all cases)</i> DATE (YYYYMMDD) 20160229																																																																																				
	b. SUBCONTRACT NUMBER			b. REVISED <i>(Supersedes all previous specs)</i>	REVISION NO. DATE (YYYYMMDD)																																																																																				
	c. SOLICITATION OR OTHER NUMBER		DUE DATE (YYYYMMDD)	c. FINAL <i>(Complete item 5 in all cases)</i> DATE (YYYYMMDD)																																																																																					
4. IS THIS A FOLLOW-ON CONTRACT?																																																																																									
		YES	☒	NO If Yes, complete the following:																																																																																					
Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.																																																																																									
5. IS THIS A FINAL DD FORM 254?																																																																																									
		YES	☒	NO If Yes, complete the following:																																																																																					
In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.																																																																																									
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>																																																																																									
a. NAME, ADDRESS, AND ZIP CODE Schafer Corporation 3811 N. Fairfax Dr., Ste. 400 Arlington, VA 22203		b. CAGE CODE 9M027		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> Alexandria Field Office Email: Crystalcity.IOFCK1@dss.mil Phone: 571-551-7920																																																																																					
7. SUBCONTRACTOR																																																																																									
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>																																																																																					
8. ACTUAL PERFORMANCE																																																																																									
a. LOCATION Defense Advanced Research Projects Agency (DARPA) 675 N. Randolph St. Arlington, VA 22203		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>																																																																																					
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Biological Technologies Office - Systems, Engineering, and Technical Assistance Support																																																																																									
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 60%;">10. CONTRACTOR WILL REQUIRE ACCESS TO:</th> <th style="width: 5%;">YES</th> <th style="width: 5%;">NO</th> <th style="width: 20%;">11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</th> <th style="width: 5%;">YES</th> <th style="width: 5%;">NO</th> </tr> <tr> <td>a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION</td> <td style="text-align: center;">☒</td> <td style="text-align: center;">☐</td> <td>a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> </tr> <tr> <td>b. RESTRICTED DATA</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> <td>b. RECEIVE CLASSIFIED DOCUMENTS ONLY</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> </tr> <tr> <td>c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> <td>c. RECEIVE AND GENERATE CLASSIFIED MATERIAL</td> <td style="text-align: center;">☒</td> <td style="text-align: center;">☐</td> </tr> <tr> <td>d. FORMERLY RESTRICTED DATA</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> <td>d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> </tr> <tr> <td>e. INTELLIGENCE INFORMATION</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☐</td> <td>e. PERFORM SERVICES ONLY</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> </tr> <tr> <td>(1) Sensitive Compartmented Information (SCI)</td> <td style="text-align: center;">☒</td> <td style="text-align: center;">☐</td> <td>f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> </tr> <tr> <td>(2) Non-SCI</td> <td style="text-align: center;">☒</td> <td style="text-align: center;">☐</td> <td>g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> </tr> <tr> <td>f. SPECIAL ACCESS INFORMATION</td> <td style="text-align: center;">☒</td> <td style="text-align: center;">☐</td> <td>h. REQUIRE A COMSEC ACCOUNT</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> </tr> <tr> <td>g. NATO INFORMATION</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> <td>i. HAVE TEMPEST REQUIREMENTS</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> </tr> <tr> <td>h. FOREIGN GOVERNMENT INFORMATION</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> <td>j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS</td> <td style="text-align: center;">☒</td> <td style="text-align: center;">☐</td> </tr> <tr> <td>i. LIMITED DISSEMINATION INFORMATION</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> <td>k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE</td> <td style="text-align: center;">☐</td> <td style="text-align: center;">☒</td> </tr> <tr> <td>l. FOR OFFICIAL USE ONLY INFORMATION</td> <td style="text-align: center;">☒</td> <td style="text-align: center;">☐</td> <td>l. OTHER <i>(Specify)</i></td> <td></td> <td></td> </tr> <tr> <td>k. OTHER <i>(Specify)</i> ACCM</td> <td style="text-align: center;">☒</td> <td style="text-align: center;">☐</td> <td></td> <td></td> <td style="text-align: center;">☒</td> </tr> </table>						10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO	a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	☒	☐	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	☐	☒	b. RESTRICTED DATA	☐	☒	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	☐	☒	c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	☐	☒	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	☒	☐	d. FORMERLY RESTRICTED DATA	☐	☒	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	☐	☒	e. INTELLIGENCE INFORMATION	☐	☐	e. PERFORM SERVICES ONLY	☐	☒	(1) Sensitive Compartmented Information (SCI)	☒	☐	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	☐	☒	(2) Non-SCI	☒	☐	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	☐	☒	f. SPECIAL ACCESS INFORMATION	☒	☐	h. REQUIRE A COMSEC ACCOUNT	☐	☒	g. NATO INFORMATION	☐	☒	i. HAVE TEMPEST REQUIREMENTS	☐	☒	h. FOREIGN GOVERNMENT INFORMATION	☐	☒	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	☒	☐	i. LIMITED DISSEMINATION INFORMATION	☐	☒	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	☐	☒	l. FOR OFFICIAL USE ONLY INFORMATION	☒	☐	l. OTHER <i>(Specify)</i>			k. OTHER <i>(Specify)</i> ACCM	☒	☐			☒
10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO																																																																																				
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	☒	☐	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	☐	☒																																																																																				
b. RESTRICTED DATA	☐	☒	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	☐	☒																																																																																				
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	☐	☒	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	☒	☐																																																																																				
d. FORMERLY RESTRICTED DATA	☐	☒	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	☐	☒																																																																																				
e. INTELLIGENCE INFORMATION	☐	☐	e. PERFORM SERVICES ONLY	☐	☒																																																																																				
(1) Sensitive Compartmented Information (SCI)	☒	☐	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	☐	☒																																																																																				
(2) Non-SCI	☒	☐	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	☐	☒																																																																																				
f. SPECIAL ACCESS INFORMATION	☒	☐	h. REQUIRE A COMSEC ACCOUNT	☐	☒																																																																																				
g. NATO INFORMATION	☐	☒	i. HAVE TEMPEST REQUIREMENTS	☐	☒																																																																																				
h. FOREIGN GOVERNMENT INFORMATION	☐	☒	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	☒	☐																																																																																				
i. LIMITED DISSEMINATION INFORMATION	☐	☒	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	☐	☒																																																																																				
l. FOR OFFICIAL USE ONLY INFORMATION	☒	☐	l. OTHER <i>(Specify)</i>																																																																																						
k. OTHER <i>(Specify)</i> ACCM	☒	☐			☒																																																																																				

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)

No information, except as provided in applicable U.S. Statutes, which is classified or unclassified pertaining to this contract shall be released for public dissemination without prior written approval of DARPA.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

10a: Classified COMSEC information/material will be protected IAW DoD 5220.22-M. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. In accordance with DoD 5220.22-M (9-407), further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior written approval of the DARPA, Contracting Officer for Security Matters. (ref. DoD 5220.22-M (Ch 9, Sec 4))

All Contractors performing on this contract shall abide by all current and applicable successor governmental guidance. Please contact your FSO, PSO or PSR if any questions arise pertaining to the availability of these guidance documents."

All Contractors performing on this contract shall abide by the Open Skies Treaty or other U.S. on-site treaty compliance obligations. In doing so, the Contractor may be required to create and execute treaty compliance plans. These plans must be approved by the cognizant Program Security Officer.

Reports of loss, compromise or suspected compromise shall be provided to the appropriate DARPA Program Security Officer (PSO) within 24 hours of the incident, in addition to the reporting requirements to DSS outlined in the NISPOM.

All of the above security requirements, where applicable, will flow down to any subcontractors and consultants supporting this contract. Copies of all subcontractor DD 254's should be emailed to the DARPA Classification Management Office, (b)(6)@darpa.mil.

Biological Technologies Office POCs: (b)(6)

---See Continuation Sheet---

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirement to the cognizant security office. Use item 13 if additional space is needed.)

When information is controlled by the United States Munitions List (USML), the contractor must abide by the International Traffic Arms Regulation (ITAR) requirements. Program information shall be protected in accordance with various DARPA and other agency security classification guidance, to be provided by cognizant DARPA PSO(s).

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use item 13 if additional space is needed.)

DARPA is responsible for inspection of all SAP materials under this contract. DIA is responsible for inspection of all SCI materials under this contract, IAW the DARPA/DSS MOU dated June 20, 2013 DSWAN is under the security cognizance of DARPA and may include visits from DARPA DSWAN security to validate the secure operating status.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

b. TITLE

c. TELEPHONE (Include Area Code)

(b)(6)

(b)(6)

d. ADDRESS (include Zip Code)

Defense Advanced Research Projects Agency (DARPA)
675 North Randolph Street
Arlington, VA 22203

(b)(6)

17. REQUIRED DISTRIBUTION

- ☒ a. CONTRACTOR
- ☐ b. SUBCONTRACTOR
- ☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
- ☒ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
- ☒ e. ADMINISTRATIVE CONTRACTING OFFICER
- ☒ f. OTHERS AS NECESSARY

Designed using Adobe, DARPA/SSO

CONTINUATION SHEET FOR DD 254, CONTRACT SECURITY CLASSIFICATION SPECIFICATION

CONTRACT NUMBER
D16PC00069

Block 13: (Continued)

10e(1): SCI Access required. The Director, DIA and Director, DARPA, have exclusive security responsibility for SCI released to the contractor or developed under this contract. Before releasing or providing SCI to contractor personnel, the GCA shall ensure that they are appropriately cleared in accordance with ICD 704, and they agree to follow controls and procedures for the protection, handling, and accountability of SCI. All activities involving SCI (including discussions) shall be conducted in sensitive compartmented information facilities (SCIFs). Physical security standards for SCIFs are contained in ICD 705 must be adhered to. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10e(2): Access to Intelligence information is required for performance. The Director, DARPA, has exclusive security responsibility for Non-SCI released to the contractor or developed under this contract. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10f: SAP activities will be accredited, governed, maintained, marked and protected in accordance with DoDM 5205.07-Volumes (1), (3) and (4); and applicable references, and program security classification guides. Access to SAP information requires employees undergo additional personnel security screening and meet the SAP access standards delineated in the applicable DoD directives and policies. SAP inspections and security oversight while in component facilities are under the cognizance of the DARPA SAPCO, as appropriate. The performer is required to submit an accreditation package (Fixed Facility Checklists (FFC) and other applicable documents) and/or System Security Plans (SSP) to the responsible DARPA PSO via "DFASTS." Otherwise, contact your PSO for submission instructions.

Effective May 1, 2015 Program Access Request (PAR) packages will be coordinated using the recently approved PAR and PSQ templates. The approved templates can be found at <http://www.dss.mil/isp/templates.html>.

All Special Access Program (SAP) accredited areas must meet the minimum physical and technical security standards outlined in the DoD 5205.07 SAP Manual Volume 3 and its references in Enclosure 1, before receiving, generating, processing, using, or storing SAP classified information, as appropriate to the accreditation. New SAP accredited areas will be inspected by DARPA physical security prior to accreditation. In accordance with DoDM 5205.07-V1 (11-I), DARPA PSO review is required prior to release to subcontractors. (ref. DoDM 5205.07-Volumes (1), (3) and (4))

10j: For Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in DoD Manual 5200.01 Volume 4, DoD Information Security Program.

10k: Alternative Compensatory Control Measures (ACCM) referenced on DARPA-associated contract DD Forms 254 are established, controlled, managed, and administered by non-DARPA Department of Defense (DoD) entities. Access may be provided by DARPA, but all guidance relating to these ACCM procedures and reporting are the responsibility of the establishing DoD entity.

11e: The contractor requires access to classified source data up to and including Top Secret in support of the work effort. Classified material generated in support of this contract shall be classified in accordance with the source material used or DARPA security classification guidance, which will be provided by the DARPA Program Security Officer or the Program Security Representative. Automated information systems must be certified and accredited by the cognizant security agency prior to processing classified information for a DARPA program. All personnel performing Information Assurance (IA)/cybersecurity related duties on DARPA accredited classified information systems shall meet the requirements set forth in DoD 8570.01-M "Information Assurance Workforce Improvement Program." All classified information received or generated under this contract is the property of the U.S. Government. At the termination or expiration of this contract, DARPA will be contacted for proper disposition instructions. SAP information systems will require an authorization-to-operate using the Risk Management Framework (RMF) process outlined in the "Joint Special Access Program (SAP) Implementation Guide (JSIG)", Revision 3, dated October 9, 2013 (or successor document).

11j: The contractor must abide by guidance outlined in the DARPA Security Guide, as well as, the DARPA Baseline Agency OPSEC Plan, which will be provided by the PSO or PSR.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED TOP SECRET b. LEVEL OF SAFEGUARD REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)			3. THIS SPECIFICATION IS: (X and complete as applicable)		
X	a. PRIME CONTRACT NUMBER D16PC00069		a. ORIGINAL (Complete date in all cases)		DATE (YYYYMMDD) 20160229
	b. SUBCONTRACT NUMBER		X	b. REVISED (Supersedes all previous specs)	REVISION NO. 1 DATE (YYYYMMDD) 20160608
	c. SOLICITATION OR OTHER NUMBER	DUE DATE (YYYYMMDD)	c. FINAL (Complete Item 5 in all cases)		DATE (YYYYMMDD)
4. IS THIS A FOLLOW-ON CONTRACT?					
		☐ YES	☒ NO	If Yes, complete the following:	
Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254?					
		☐ YES	☒ NO	If Yes, complete the following:	
In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.					
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)					
a. NAME, ADDRESS, AND ZIP CODE Schafer Government Services, LLC 3811 North Fairfax Drive, Suite 400 Arlington, VA 22203		b. CAGE CODE 9M027		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) Defense Security Service (DSS) Alexandria 1 Field Office (IOFCS1) Crystalcity IOFCK1@dss.mil	
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
8. ACTUAL PERFORMANCE					
a. LOCATION Defense Advanced Research Projects Agency (DARPA) 675 N. Randolph St. Arlington, VA 22203-2114		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Biological Technologies Office (BTO) - Systems, Engineering, and Technical Assistance (SETA) support					
10. CONTRACTOR WILL REQUIRE ACCESS TO:					
	YES	NO			YES
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		X
b. RESTRICTED DATA		X			X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X			X
d. FORMERLY RESTRICTED DATA		X			X
e. INTELLIGENCE INFORMATION					X
(1) Sensitive Compartmented Information (SCI)	X				X
(2) Non-SCI	X				X
f. SPECIAL ACCESS INFORMATION	X				X
g. NATO INFORMATION		X			X
h. FOREIGN GOVERNMENT INFORMATION		X			X
i. LIMITED DISSEMINATION INFORMATION		X	X		
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER (Specify)		
k. OTHER (Specify) ACCM		X			

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)

No information, except as provided in applicable U.S. Statutes, which is classified or unclassified pertaining to this contract shall be released for public dissemination without prior written approval of DARPA.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Contract Number D16PC00069

All Contractors performing on this contract shall abide by all current and applicable successor governmental guidance. Please contact your FSO, PSO or PSR if any questions arise pertaining to the availability of these guidance documents.

All Contractors performing on this contract shall abide by the Open Skies Treaty or other U.S. on-site treaty compliance obligations. In doing so, the Contractor may be required to create and execute treaty compliance plans. These plans must be approved by the cognizant Program Security Officer.

Reports of loss, compromise or suspected compromise shall be provided to the appropriate DARPA Program Security Officer (PSO) within 24 hours of the incident, in addition to the reporting requirements to DSS outlined in the NISPOM.

All of the above security requirements, where applicable, will flow down to any subcontractors and consultants supporting this contract. Copies of all subcontractor DD 254's should be emailed to the DARPA Classification Management Office (b)(6)@darpa.mil.

BTO POCs: (b)(6)

See Continuation Page

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirement to the cognizant security office. Use Item 13 if additional space is needed.)

When information is controlled by the United States Munitions List (USML), the contractor must abide by the International Traffic Arms Regulation (ITAR) requirements. Program information shall be protected in accordance with various DARPA and other agency security classification guidance, to be provided by cognizant DARPA PSO(s). The Collateral Secret DARPA Secure Wide Area Network (DSWAN) will be operated IAW the attached DARPA/DSS MOU dated June 20, 2013.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

DARPA is responsible for inspection of all SAP materials under this contract.

DIA is responsible for inspection of all SCI materials under this contract.

IAW the DARPA/DSS MOU dated June 20, 2013 DSWAN is under the security cognizance of DARPA and may include visits from DARPA DSWAN security to validate the secure operating status.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

(b)(6)

b. TITLE

(b)(6)

c. TELEPHONE (Include Area Code)

(b)(6)

d. ADDRESS
Defense A
675 North
Arlington,

e. SIGNATURE

DARPA)

17. REQUIRED DISTRIBUTION

- ☒ a. CONTRACTOR
☐ b. SUBCONTRACTOR
☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
☒ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
☒ e. ADMINISTRATIVE CONTRACTING OFFICER
☒ f. OTHERS AS NECESSARY

CONTINUATION SHEET FOR DD 254, CONTRACT SECURITY CLASSIFICATION SPECIFICATION

CONTRACT NUMBER
D16PC00069

10a: Classified COMSEC information/material will be protected IAW DoD 5220.22-M. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. In accordance with DoD5220.22-M (9-407), further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior written approval of the DARPA, Contracting Officer for Security Matters. (ref. DoD 5220.22-M (Ch 9, Sec 4))

10e(1): SCI Access required. The Director, DIA and Director, DARPA, have exclusive security responsibility for SCI released to the contractor or developed under this contract. Before releasing or providing SCI to contractor personnel, the GCA shall ensure that they are appropriately cleared in accordance with ICD 704, and they agree to follow controls and procedures for the protection, handling, and accountability of SCI. All activities involving SCI (including discussions) shall be conducted in sensitive compartmented information facilities (SCIFs). Physical security standards for SCIFs are contained in ICD 705 must be adhered to. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10e(2): Access to Intelligence information is required for performance. The Director, DARPA, has exclusive security responsibility for Non-SCI released to the contractor or developed under this contract. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10f: SAP activities will be accredited, governed, maintained, marked and protected in accordance with DoDM 5205.07-Volumes (1), (3) and (4); and applicable references, and program security classification guides. Access to SAP information requires employees undergo additional personnel security screening and meet the SAP access standards delineated in the applicable DoD directives and policies. SAP inspections and security oversight while in component facilities are under the cognizance of the DARPA SAPCO, as appropriate. The performer is required to submit an accreditation package (Fixed Facility Checklists (FFC) and other applicable documents) and/or System Security Plans (SSP) to the responsible DARPA PSO via "DFASTS." Otherwise, contact your PSO for submission instructions.

Effective May 1, 2015 Program Access Request (PAR) packages will be coordinated using the recently approved PAR and PSQ templates. The approved templates can be found at <http://www.dss.mil/isp/templates.html>.

All Special Access Program (SAP) accredited areas must meet the minimum physical and technical security standards outlined in the DoD 5205.07 SAP Manual Volume 3 and its references in Enclosure 1, before receiving, generating, processing, using, or storing SAP classified information, as appropriate to the accreditation. New SAP accredited areas will be inspected by DARPA physical security prior to accreditation. In accordance with DoDM 5205.07-V1 (11-1), DARPA PSO review is required prior to release to subcontractors. (ref. DoDM 5205.07-Volumes (1), (3) and (4))

10j: For Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in DoD Manual 5200.01 Volume 4, DoD Information Security Program.

10k: Alternative Compensatory Control Measures (ACCM) referenced on DARPA-associated contract DD Forms 254 are established, controlled, managed, and administered by non-DARPA Department of Defense (DoD) entities. Access may be provided by DARPA, but all guidance relating to these ACCM procedures and reporting are the responsibility of the establishing DoD entity.

11c: The contractor requires access to classified source data up to and including Top Secret in support of the work effort. Classified material generated in support of this contract shall be classified in accordance with the source material used or DARPA security classification guidance, which will be provided by the DARPA Program Security Officer or the Program Security Representative. Automated information systems must be certified and accredited by the cognizant security agency prior to processing classified information for a DARPA program. All personnel performing Information Assurance (IA)/cybersecurity related duties on DARPA accredited classified information systems shall meet the requirements set forth in DoD 8570.01-M "Information Assurance Workforce Improvement Program." All classified information received or generated under this contract is the property of the U.S. Government. At the termination or expiration of this contract, DARPA will be contacted for proper disposition instructions. SAP information systems will require an authorization-to-operate using the Risk Management Framework (RMF) process outlined in the "Joint Special Access Program (SAP) Implementation Guide (JSIG)", Revision 3, dated October 9, 2013 (or successor document).

11j: The contractor must abide by guidance outlined in the DARPA Security Guide, as well as, the DARPA Baseline Agency OPSEC Plan, which will be provided by the PSO or PSR.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION (The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED TOP SECRET b. LEVEL OF SAFEGUARD REQUIRED NONE			
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)				3. THIS SPECIFICATION IS: (X and complete as applicable)			
X a. PRIME CONTRACT NUMBER D16PC00069				a. ORIGINAL (Complete date in all cases)		DATE (YYYYMMDD) 20160229	
b. SUBCONTRACT NUMBER		X		b. REVISED (Supersedes all previous specs)	REVISION NO. 2	DATE (YYYYMMDD) 20171101	
c. SOLICITATION OR OTHER NUMBER		DUE DATE (YYYYMMDD)		c. FINAL (Complete Item 5 in all cases)		DATE (YYYYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? YES X NO If Yes, complete the following: Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.							
5. IS THIS A FINAL DD FORM 254? YES X NO If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____							
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)							
a. NAME, ADDRESS, AND ZIP CODE Schafer Government Services, LLC 3811 North Fairfax Drive, Suite 400 Arlington, VA 22203		b. CAGE CODE 9M027		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) Alexandria I Field Office (IOFCS1) DSS.Alexandria1@mail.mil 571-551-7920			
7. SUBCONTRACTOR							
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)			
8. ACTUAL PERFORMANCE							
a. LOCATION Defense Advanced Research Project Agency (DARPA) 675 N. Randolph St. Arlington, VA 22203		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)			
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Biological Technologies Office - Systems, Engineering and Technical Assistance (SETA) Support.							
10. CONTRACTOR WILL REQUIRE ACCESS TO:							
11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:							
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X	
b. RESTRICTED DATA		X		b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X		c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		X	
d. FORMERLY RESTRICTED DATA		X		d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X	
e. INTELLIGENCE INFORMATION		X		e. PERFORM SERVICES ONLY		X	
(1) Sensitive Compartmented Information (SCI)		X		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X	
(2) Non-SCI		X		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X	
f. SPECIAL ACCESS INFORMATION		X		h. REQUIRE A COMSEC ACCOUNT		X	
g. NATO INFORMATION		X		i. HAVE TEMPEST REQUIREMENTS		X	
h. FOREIGN GOVERNMENT INFORMATION		X		j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X	
i. LIMITED DISSEMINATION INFORMATION		X		k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X	
j. FOR OFFICIAL USE ONLY INFORMATION		X		l. OTHER (Specify)			
k. OTHER (Specify) *ACCM		X				X	

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

☐ Direct

☒ Through (Specify)

No information, except as provided in applicable U.S. Statutes, which is classified of unclassified pertaining to this contract shall be released for public dissemination without prior written approval of DARPA.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Contract # D16PC00069.

8a: The contractor is authorized to work at the following facility up to the Top Secret level.
(ref. DoDM5220.22-M (2-100a))

10a: Classified COMSEC information/material will be protected IAW DoD 5220.22-M. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. In accordance with DoD5220.22-M (9-407), further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior written approval of the DARPA, Contracting Officer for Security Matters. (ref. DoD 5220.22-M (Ch 9, Sec 4))

10e(1): SCI Access required. The Director, DIA and Director, DARPA, have exclusive security responsibility for SCI released to the contractor or developed under this contract. Before releasing or providing SCI to contractor personnel, the GCA shall ensure that they are appropriately cleared in accordance with ICD 704, and they agree to follow controls and procedures for the protection, handling, and accountability of SCI. All activities involving SCI (including discussions) shall be conducted in sensitive compartmented information facilities (SCIFs). Physical security standards for SCIFs are contained in ICD 705 must be adhered to. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10e(2): Access to Intelligence information is required for performance. The Director, DARPA, has exclusive security responsibility for Non-SCI released to the contractor or developed under this contract. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract.

☒ Yes

☐ No

(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirement to the cognizant security office. Use Item 13 if additional space is needed.)

Program information shall be protected in accordance with various DARPA and other agency security classification guidance, to be provided by cognizant DARPA PSO(s).

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office.

☒ Yes

☐ No

(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

SAP: DARPA is responsible for inspection of all SAP materials under this contract.

SCI: DIA is responsible for inspection of all SCI materials under this contract.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

(b)(6)

b. TITLE

(b)(6)

c. TELEPHONE (Include Area Code)

(b)(6)

d. ADDRESS (Include Zip Code)

Defense Advanced Research Project Agency
675 n. Rar(b)(6)
Arlington,

e. SIGNA

17. REQUIRED DISTRIBUTION

☒ a. CONTRACTOR

☐ b. SUBCONTRACTOR

☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR

☒ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION

☒ e. ADMINISTRATIVE CONTRACTING OFFICER

☒ f. OTHERS AS NECESSARY

UNCLASSIFIED

CONTINUATION SHEET FOR DD 254, CONTRACT SECURITY CLASSIFICATION SPECIFICATION

CONTRACT NUMBER
D16PC00069

10f: SAP activities will be accredited, governed, maintained, marked and protected in accordance with DoDM 5205.07-Volumes (1), (3) and (4); and applicable references, and program security classification guides. Access to SAP information requires employees undergo additional personnel security screening and meet the SAP access standards delineated in the applicable DoD directives and policies. SAP inspections and security oversight while in component facilities are under the cognizance of the DARPA SAPCO, as appropriate. The performer is required to submit an accreditation package (Fixed Facility Checklists (FFC) and other applicable documents) and/or System Security Plans (SSP) to the responsible DARPA PS via "DFASTS." Otherwise, contact your PSO for submission instructions.

Effective May 1, 2015 Program Access Request (PAR) packages will be coordinated using the recently approved PAR and PSQ templates. The approved templates can be found at <http://www.dss.mil/isp/templates.html>.

All Special Access Program (SAP) accredited areas must meet the minimum physical and technical security standards outlined in the DoD 5205.07 SAP Manual Volume 3 and its references in Enclosure 1, before receiving, generating, processing, using, or storing SAP classified information, as appropriate to the accreditation. New SAP accredited areas will be inspected by DARPA physical security prior to accreditation. In accordance with DoDM 5205.07-V1 (11-1), DARPA PSO review is required prior to release to subcontractors. (ref. DoDM 5205.07-Volumes (1), (3) and (4))

10j: For Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in DoD Manual 5200.01 Volume 4, DoD Information Security Program.

10k: Alternative Compensatory Control Measures (ACCM) referenced on DARPA-associated contract DD Forms 254 are established, controlled, managed, and administered by non-DARPA Department of Defense (DoD) entities. Access may be provided by DARPA, but all guidance relating to these ACCM procedures and reporting are the responsibility of the establishing DoD entity.

11a: Contractor performance is restricted to another contractor's facility or Government facility. Contractor has NO storage requirement. DARPA or prime contractor will provide security classification guidance for the performance of this contract.

11c: The contractor requires access to classified source data up to and including Top Secret in support of the work effort. Classified material generated in support of this contract shall be classified in accordance with the source material used or DARPA security classification guidance, which will be provided by the DARPA Program Security Officer or the Program Security Representative. Automated information systems must be certified and accredited by the cognizant security agency prior to processing classified information for a DARPA program. All personnel performing Information Assurance (IA)/cybersecurity related duties on DARPA accredited classified information systems shall meet the requirements set forth in DoD Directive 8140.01, "Cyberspace Workforce Management." All classified information received or generated under this contract is the property of the U.S. Government. At the termination or expiration of this contract, DARPA will be contacted for proper disposition instructions.

11j: The contractor must abide by guidance outlined in the DARPA Security Guide, as well as, the DARPA Baseline Agency OPSEC Plan, which will be provided by the PSO or PSR.

All Contractors performing on this contract shall abide by all current and applicable successor governmental guidance. Please contact your FSO, PSO, or PSR if any questions arise pertaining to the availability of these guidance documents.

All Contractors performing on this contract shall abide by the Open Skies Treaty or other U.S. on-site treaty compliance obligations. In doing so, the Contractor may be required to create and execute treaty compliance plans. These plans must be approved by the cognizant Program Security Officer.

Reports of loss, compromise, or suspected compromise shall be provided to the appropriate DARPA Program Security Officer (PSO) within 24 hours of the incident, in addition to the reporting requirements to DSS outlined in the NISPOM.

All of the above security requirements, where applicable, will flow down to any subcontractors and consultants supporting this contract. Copies of all subcontractor DD 254's should be emailed to the DARPA Industrial Security Office, (b)(6)@darpa.mil.

Biological Technologies Office (b)(6)

UNCLASSIFIED

Designed using Adobe, DARPA/MSO

CONTINUATION SHEET FOR DD 254, CONTRACT SECURITY CLASSIFICATION SPECIFICATION

CONTRACT NUMBER
D16PC00069

SAVANNAH is the DARPA SAP enterprise information system solution and may be deployed for program support. SAVANNAH can be used to extend existing program networks to improve secure information flow between DARPA and performer sites via a "Single Level Connection." An evaluation of performer requirements concerning "Single Level Connections" is required for prudent use of SAVANNAH capabilities. DARPA AO/DAOs and SCAs will provide guidance on Single Level Connection capabilities and the "Connection Approval Package (CAP)."

SAP information systems will require an authorization-to-operate using the Risk Management Framework (RMF) process outlined in the "Joint Special Access Program Implementation Guide (JSIG), dated April 1, 2016" (or successor document).

SAP information systems utilizing Windows as their operating system must utilize the Windows 10 solution. Information regarding the correct Windows 10 version or its successor will be disseminated by the DARPA PSO or your Cybersecurity System Control Assessor (SCA).

Data Transfers: Data transfers will be performed IAW the processes and procedures outlined in the "DARPA Data Transfer SOP," April 11, 2016, Version 1.4 (or most recent version).

Media Encryption: After October 1, 2017, all portable SAP media must be encrypted. Encryption of Data at Rest shall be implemented on SAP IT IAW DoD SAP CIO specified system type deadlines using NSA approved or FIPS 140-2 compliant products.

SAP IT Disposition: The disposition (e.g., sanitization, destruction and release) of SAP IT by contractors will follow the guidelines outlined in "OSD SAPCO, Disposition of DoD Special Access Program Information Technology Devices," July 27, 2017, to include any follow on OSD SAPCO or OSD SAP CIO guidance or directives that supersede this memorandum. DARPA will keep industry partners updated through their PSOs to ensure most current OSD Directives or Instruction flow down.

SAP IT Assessments will be required of DARPA accredited SAP IT systems. Assessments include but are not limited to the SAP IT Census and SAP IT Scorecard. These assessments are critical in ensuring the size, scope, and complexity of our SAP IT systems are properly recorded, managed, and supported.

Additional SAP related security policy documents may be disseminated via the DARPA PSO IAW applicable statutes, Executive orders, cognizant security agency directives, instructions, manuals, regulations, and memorandums. When this documentation is modified, revised, supplemented, changed or reissued, it constitutes implementable security guidance IAW established effective dates. In cases of doubt over the specific provisions, the contractor should consult the PSO and the Contracting Officer before taking any action or expending program-related funds.

Prime Contractors are required to flow down applicable security policy to their sub-contractors as soon as possible, not to exceed 30 calendar days, of receipt of this guidance.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED TOP SECRET b. LEVEL OF SAFEGUARD REQUIRED NONE																																																																																					
2. THIS SPECIFICATION IS FOR: (X and complete as applicable) X a. PRIME CONTRACT NUMBER D16PC00068 b. SUBCONTRACT NUMBER c. SOLICITATION OR OTHER NUMBER DUE DATE (YYYYMMDD)			3. THIS SPECIFICATION IS: (X and complete as applicable) X a. ORIGINAL (Complete date in all cases) DATE (YYYYMMDD) 20160129 b. REVISED (Supersedes all previous specs) REVISION NO. DATE (YYYYMMDD) c. FINAL (Complete item 5 in all cases) DATE (YYYYMMDD)																																																																																						
4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☒ NO If Yes, complete the following: Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.																																																																																									
5. IS THIS A FINAL DD FORM 254? ☐ YES ☒ NO If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.																																																																																									
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code) a. NAME, ADDRESS, AND ZIP CODE Booz Allen Hamilton 8283 Greensboro Dr. McLean, VA 22102 b. CAGE CODE 17038 c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) Chantilly Field Office Email: CHANTILLY.IOFCCI@DSS.MIL Phone: 703-428-0018																																																																																									
7. SUBCONTRACTOR a. NAME, ADDRESS, AND ZIP CODE b. CAGE CODE c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)																																																																																									
8. ACTUAL PERFORMANCE a. LOCATION Defense Advanced Research Projects Agency (DARPA) 675 N. Randolph St. Arlington, VA 22203 b. CAGE CODE c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)																																																																																									
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Biological Technologies Office - Systems, Engineering and Technical Assistance Support																																																																																									
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 40%;">10. CONTRACTOR WILL REQUIRE ACCESS TO:</th> <th style="width: 5%;">YES</th> <th style="width: 5%;">NO</th> <th style="width: 40%;">11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</th> <th style="width: 5%;">YES</th> <th style="width: 5%;">NO</th> </tr> <tr> <td>a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION</td> <td style="text-align: center;">X</td> <td></td> <td>a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY</td> <td></td> <td style="text-align: center;">X</td> </tr> <tr> <td>b. RESTRICTED DATA</td> <td></td> <td style="text-align: center;">X</td> <td>b. RECEIVE CLASSIFIED DOCUMENTS ONLY</td> <td></td> <td style="text-align: center;">X</td> </tr> <tr> <td>c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION</td> <td></td> <td style="text-align: center;">X</td> <td>c. RECEIVE AND GENERATE CLASSIFIED MATERIAL</td> <td style="text-align: center;">X</td> <td></td> </tr> <tr> <td>d. FORMERLY RESTRICTED DATA</td> <td></td> <td style="text-align: center;">X</td> <td>d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE</td> <td></td> <td style="text-align: center;">X</td> </tr> <tr> <td>e. INTELLIGENCE INFORMATION</td> <td></td> <td></td> <td>e. PERFORM SERVICES ONLY</td> <td></td> <td style="text-align: center;">X</td> </tr> <tr> <td>(1) Sensitive Compartmented Information (SCI)</td> <td style="text-align: center;">X</td> <td></td> <td>f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES</td> <td></td> <td style="text-align: center;">X</td> </tr> <tr> <td>(2) Non-SCI</td> <td style="text-align: center;">X</td> <td></td> <td>g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER</td> <td></td> <td style="text-align: center;">X</td> </tr> <tr> <td>f. SPECIAL ACCESS INFORMATION</td> <td style="text-align: center;">X</td> <td></td> <td>h. REQUIRE A COMSEC ACCOUNT</td> <td></td> <td style="text-align: center;">X</td> </tr> <tr> <td>g. NATO INFORMATION</td> <td></td> <td style="text-align: center;">X</td> <td>i. HAVE TEMPEST REQUIREMENTS</td> <td></td> <td style="text-align: center;">X</td> </tr> <tr> <td>h. FOREIGN GOVERNMENT INFORMATION</td> <td></td> <td style="text-align: center;">X</td> <td>j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS</td> <td style="text-align: center;">X</td> <td></td> </tr> <tr> <td>i. LIMITED DISSEMINATION INFORMATION</td> <td></td> <td style="text-align: center;">X</td> <td>k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE</td> <td></td> <td style="text-align: center;">X</td> </tr> <tr> <td>j. FOR OFFICIAL USE ONLY INFORMATION</td> <td style="text-align: center;">X</td> <td></td> <td>l. OTHER (Specify)</td> <td></td> <td></td> </tr> <tr> <td>k. OTHER (Specify)</td> <td></td> <td style="text-align: center;">X</td> <td></td> <td></td> <td style="text-align: center;">X</td> </tr> </table>						10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO	a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X	b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X	c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X		d. FORMERLY RESTRICTED DATA		X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X	e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY		X	(1) Sensitive Compartmented Information (SCI)	X		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X	(2) Non-SCI	X		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X	f. SPECIAL ACCESS INFORMATION	X		h. REQUIRE A COMSEC ACCOUNT		X	g. NATO INFORMATION		X	i. HAVE TEMPEST REQUIREMENTS		X	h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X		i. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X	j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER (Specify)			k. OTHER (Specify)		X			X
10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO																																																																																				
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X																																																																																				
b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X																																																																																				
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X																																																																																					
d. FORMERLY RESTRICTED DATA		X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X																																																																																				
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY		X																																																																																				
(1) Sensitive Compartmented Information (SCI)	X		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X																																																																																				
(2) Non-SCI	X		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X																																																																																				
f. SPECIAL ACCESS INFORMATION	X		h. REQUIRE A COMSEC ACCOUNT		X																																																																																				
g. NATO INFORMATION		X	i. HAVE TEMPEST REQUIREMENTS		X																																																																																				
h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X																																																																																					
i. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X																																																																																				
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER (Specify)																																																																																						
k. OTHER (Specify)		X			X																																																																																				

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)

No information, except as provided in applicable U.S. Statutes, which is classified or unclassified pertaining to this contract shall be released for public dissemination without prior written approval of DARPA.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

10a: Classified COMSEC information/material will be protected IAW DoD 5220.22-M. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. In accordance with DoD 5220.22-M (9-407), further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior written approval of the DARPA, Contracting Officer for Security Matters. (ref. DoD 5220.22-M (Ch 9, Sec 4))

All Contractors performing on this contract shall abide by all current and applicable successor governmental guidance. Please contact your FSO, PSO or PSR if any questions arise pertaining to the availability of these guidance documents."

All Contractors performing on this contract shall abide by the Open Skies Treaty or other U.S. on-site treaty compliance obligations. In doing so, the Contractor may be required to create and execute treaty compliance plans. These plans must be approved by the cognizant Program Security Officer.

Reports of loss, compromise or suspected compromise shall be provided to the appropriate DARPA Program Security Officer (PSO) within 24 hours of the incident, in addition to the reporting requirements to DSS outlined in the NISPOM.

All of the above security requirements, where applicable, will flow down to any subcontractors and consultants supporting this contract. Copies of all subcontractor DD 254's should be emailed to the DARPA Classification Management Office, sid-clasmgmt@darpa.mil.

Biological Technologies Office POCs: (b)(6)

---See Continuation Sheet---

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirement to the cognizant security office. Use Item 13 if additional space is needed.)

When information is controlled by the United States Munitions List (USML), the contractor must abide by the International Traffic Arms Regulation (ITAR) requirements. Program information shall be protected in accordance with various DARPA and other agency security classification guidance, to be provided by cognizant DARPA PSO(s).

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

DARPA is responsible for inspection of all SAP materials under this contract. DIA is responsible for inspection of all SCI materials under this contract. IAW the DARPA/DSS MOU dated June 20, 2013 DSWAN is under the security cognizance of DARPA and may include visits from DARPA DSWAN security to validate the secure operating status.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

b. TITLE

c. TELEPHONE (Include Area Code)

(b)(6)

d. ADDRESS (Include Zip Code)

Defense Advanced Research Projects Agency (DARPA)
675 North Randolph Street
Arlington, VA 22203

(b)(6)

17. REQUIRED DISTRIBUTION

- ☒ a. CONTRACTOR
☐ b. SUBCONTRACTOR
☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
☒ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
☒ e. ADMINISTRATIVE CONTRACTING OFFICER
☒ f. OTHERS AS NECESSARY

DD

Designed using Adobe, DARPA/SSO

CONTINUATION SHEET FOR DD 254, CONTRACT SECURITY CLASSIFICATION SPECIFICATION

CONTRACT NUMBER
D16PC00068

Block 13: (Continued)

10e(1): SCI Access required. The Director, DIA and Director, DARPA, have exclusive security responsibility for SCI released to the contractor or developed under this contract. Before releasing or providing SCI to contractor personnel, the GCA shall ensure that they are appropriately cleared in accordance with ICD 704, and they agree to follow controls and procedures for the protection, handling, and accountability of SCI. All activities involving SCI (including discussions) shall be conducted in sensitive compartmented information facilities (SCIFs). Physical security standards for SCIFs are contained in ICD 705 must be adhered to. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10e(2): Access to Intelligence information is required for performance. The Director, DARPA, has exclusive security responsibility for Non-SCI released to the contractor or developed under this contract. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10f: SAP activities will be accredited, governed, maintained, marked and protected in accordance with DoDM 5205.07-Volumes (1), (3) and (4); and applicable references, and program security classification guides. Access to SAP information requires employees undergo additional personnel security screening and meet the SAP access standards delineated in the applicable DoD directives and policies. SAP inspections and security oversight while in component facilities are under the cognizance of the DARPA SAPCO, as appropriate. The performer is required to submit an accreditation package (Fixed Facility Checklists (FFC) and other applicable documents) and/or System Security Plans (SSP) to the responsible DARPA PSO via "DFASTS." Otherwise, contact your PSO for submission instructions.

Effective May 1, 2015 Program Access Request (PAR) packages will be coordinated using the recently approved PAR and PSQ templates. The approved templates can be found at <http://www.dss.mil/lsp/templates.html>.

All Special Access Program (SAP) accredited areas must meet the minimum physical and technical security standards outlined in the DoD 5205.07 SAP Manual Volume 3 and its references in Enclosure 1, before receiving, generating, processing, using, or storing SAP classified information, as appropriate to the accreditation. New SAP accredited areas will be inspected by DARPA physical security prior to accreditation. In accordance with DoDM 5205.07-V1 (11-1), DARPA PSO review is required prior to release to subcontractors. (ref. DoDM 5205.07-Volumes (1), (3) and (4)).

10j: For Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in DoD Manual 5200.01 Volume 4, DoD Information Security Program.

11c: The contractor requires access to classified source data up to and including Top Secret in support of the work effort. Classified material generated in support of this contract shall be classified in accordance with the source material used or DARPA security classification guidance, which will be provided by the DARPA Program Security Officer or the Program Security Representative. Automated information systems must be certified and accredited by the cognizant security agency prior to processing classified information for a DARPA program. All personnel performing Information Assurance (IA)/cyber security related duties on DARPA accredited classified information systems shall meet the requirements set forth in DoD 8570.01-M "Information Assurance Workforce Improvement Program." All classified information received or generated under this contract is the property of the U.S. Government. At the termination or expiration of this contract, DARPA will be contacted for proper disposition instructions. SAP information systems will require an authorization-to-operate using the Risk Management Framework (RMF) process outlined in the "Joint Special Access Program (SAP) Implementation Guide (JSIG)", Revision 3, dated October 9, 2013 (or successor document).

Ref 11j: The contractor must abide by guidance outlined in the DARPA Security Guide, as well as, the DARPA Baseline Agency OPSEC Plan, which will be provided by the PSO or PSR.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED TOP SECRET b. LEVEL OF SAFEGUARD REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)				3. THIS SPECIFICATION IS: (X and complete as applicable)	
☒ a. PRIME CONTRACT NUMBER D16PC00068				a. ORIGINAL (Complete date in all cases) DATE (YYYYMMDD) 20160129	
b. SUBCONTRACT NUMBER		☒ b. REVISED (Supercodes all previous specs)		REVISION NO 1 DATE (YYYYMMDD) 171017	
c. SOLICITATION OR OTHER NUMBER		DUE DATE (YYYYMMDD)		c. FINAL (Complete item 5 in all cases) DATE (YYYYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT?					
☐ YES		☒ NO If Yes, complete the following: Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.			
5. IS THIS A FINAL DD FORM 254?					
☐ YES		☒ NO If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)					
a. NAME, ADDRESS, AND ZIP CODE Booz Allen Hamilton 8283 Greensboro Dr McLean, VA 22102		b. CAGE CODE 17038		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) Chantilly Field Office Email: Chantilly.IOFCC1@dss.mil Phone: 703-428-0018	
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
8. ACTUAL PERFORMANCE					
a. LOCATION Defense Advanced Research Project Agency (DARPA) 675 N. Randolph St. Arlington, VA 22203		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Biological Technologies Office - Systems, Engineering and Technical Assistance Support					
10. CONTRACTOR WILL REQUIRE ACCESS TO:					
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		☒ YES ☐ NO		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
b. RESTRICTED DATA		☒ YES ☐ NO		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		☒ YES ☐ NO		b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
d. FORMERLY RESTRICTED DATA		☒ YES ☐ NO		c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
e. INTELLIGENCE INFORMATION		☐ YES ☐ NO		d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	
(1) Sensitive Compartmented Information (SCI)		☒ YES ☐ NO		e. PERFORM SERVICES ONLY	
(2) Non-SCI		☒ YES ☐ NO		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	
g. SPECIAL ACCESS INFORMATION		☒ YES ☐ NO		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	
h. NATO INFORMATION		☒ YES ☐ NO		h. REQUIRE A COMBID ACCOUNT	
i. FOREIGN GOVERNMENT INFORMATION		☒ YES ☐ NO		i. HAVE TEMPEST REQUIREMENTS	
j. LIMITED DISSEMINATION INFORMATION		☒ YES ☐ NO		j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	
k. FOR OFFICIAL USE ONLY INFORMATION		☒ YES ☐ NO		k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	
l. OTHER (Specify) *ACCM		☒ YES ☐ NO		l. OTHER (Specify)	

DD Form 254, DEC 1999

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Designed using Adobe, DARPA/MISO

UNCLASSIFIED // FOR OFFICIAL USE ONLY

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)

No information, except as provided in applicable U.S. Statutes, which is classified or unclassified pertaining to this contract shall be released for public dissemination without prior written approval of DARPA.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*in the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge guidance or the classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

8a: The contractor is authorized to work at the following facility up to the Secret/TS level.
(ref. DoDM5220.22-M (2-100a))

10a: Classified COMSEC information/material will be protected IAW DoD 5220.22-M. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level

10c(1): SCI Access required. The Director, DIA and Director, DARPA, have exclusive security responsibility for SCI released to the contractor or developed under this contract. Before releasing or providing SCI to contractor personnel, the GCA shall ensure that they are appropriately cleared in accordance with ICD 704, and they agree to follow controls and procedures for the protection, handling, and accountability of SCI. All activities involving SCI (including discussions) shall be conducted in sensitive compartmented information facilities (SCIFs). Physical security standards for SCIFs are contained in ICD 705 must be adhered to. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10c(2): Access to Intelligence information is required for performance. The Director, DARPA, has exclusive security responsibility for Non-SCI released to the contractor or developed under this contract. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirement to the cognizant security office. Use Item 13 if additional space is needed.)

Program information shall be protected in accordance with various DARPA and other agency security classification guidance, to be provided by cognizant DARPA PSO(s).

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

SAP: DARPA is responsible for inspection of all SAP materials under this contract.

SCI: DIA is responsible for inspection of all SCI materials under this contract.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

(b)(6)

b. TITLE

(b)(6)

c. TELEPHONE (Include Area Code)

(b)(6)

d. ADDRESS (Include Zip Code)

(b)(6)

17. REQUIRED DISTRIBUTION

- ☒ a. CONTRACTOR
☒ b. SUBCONTRACTOR
☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
☒ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
☒ e. ADMINISTRATIVE CONTRACTING OFFICER
☒ f. OTHERS AS NECESSARY

DD Form 254 (Back) DEC 1999

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Designed using Adobe, DARP/MSO

CONTINUATION SHEET FOR DD 254, CONTRACT SECURITY CLASSIFICATION SPECIFICATION

CONTRACT NUMBER D16PC00068

10f: SAP activities will be accredited, governed, maintained, marked and protected in accordance with DoDM 5205.07-Volumes (1), (3) and (4); and applicable references, and program security classification guides. Access to SAP information requires employees undergo additional personnel security screening and meet the SAP access standards delineated in the applicable DoD directives and policies. SAP inspections and security oversight while in component facilities are under the cognizance of the DARPA SAPCO, as appropriate. The performer is required to submit an accreditation package (Fixed Facility Checklists (FFC) and other applicable documents) and/or System Security Plans (SSP) to the responsible DARPA PS via "DFASTS." Otherwise, contact your PSO for submission instructions.

Effective May 1, 2015 Program Access Request (PAR) packages will be coordinated using the recently approved PAR and PSQ templates. The approved templates can be found at <http://www.dss.mil/isp/templates.html>.

All Special Access Program (SAP) accredited areas must meet the minimum physical and technical security standards outlined in the DoD 5205.07 SAP Manual Volume 3 and its references in Enclosure 1, before receiving, generating, processing, using, or storing SAP classified information, as appropriate to the accreditation. New SAP accredited areas will be inspected by DARPA physical security prior to accreditation. In accordance with DoDM 5205.07-V1 (11-1), DARPA PSO review is required prior to release to subcontractors. (ref. DoDM 5205.07-Volumes (1), (3) and (4))

10j: For Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in DoD Manual 5200.01 Volume 4, DoD Information Security Program.

10k: Alternative Compensatory Control Measures (ACCM) referenced on DARPA-associated contract DD Forms 254 are established, controlled, managed, and administered by non-DARPA Department of Defense (DoD) entities. Access may be provided by DARPA, but all guidance relating to these ACCM procedures and reporting are the responsibility of the establishing DoD entity.

11c: The contractor requires access to classified source data up to and including Top Secret in support of the work effort. Classified material generated in support of this contract shall be classified in accordance with the source material used or DARPA security classification guidance, which will be provided by the DARPA Program Security Officer or the Program Security Representative. Automated information systems must be certified and accredited by the cognizant security agency prior to processing classified information for a DARPA program. All personnel performing Information Assurance (IA)/cybersecurity related duties on DARPA accredited classified information systems shall meet the requirements set forth in DoD Directive 8140.01, "Cyberspace Workforce Management." All classified information received or generated under this contract is the property of the U.S. Government. At the termination or expiration of this contract, DARPA will be contacted for proper disposition instructions.

11j: The contractor must abide by guidance outlined in the DARPA Security Guide, as well as, the DARPA Baseline Agency OPSEC Plan, which will be provided by the PSO or PSR.

Biological Technologies Office POCs (b)(6)

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION (The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED TOP SECRET b. LEVEL OF SAFEGUARD REQUIRED NONE			
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)				3. THIS SPECIFICATION IS: (X and complete as applicable)			
X a. PRIME CONTRACT NUMBER D16PC00068				a. ORIGINAL (Complete date in all cases) DATE (YYYYMMDD) 20160129			
b. SUBCONTRACT NUMBER		X		b. REVISED (Supersedes all previous specs) 2	REVISION NO. DATE (YYYYMMDD) 20171101		
c. SOLICITATION OR OTHER NUMBER		DUE DATE (YYYYMMDD)		c. FINAL (Complete Item 5 in all cases) DATE (YYYYMMDD)			
4. IS THIS A FOLLOW-ON CONTRACT? YES X NO If Yes, complete the following: Classified material received or generated under (Preceding Contract Number) is transferred to this follow-on contract.							
5. IS THIS A FINAL DD FORM 254? YES X NO If Yes, complete the following: In response to the contractor's request dated , retention of the classified material is authorized for the period of							
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)							
a. NAME, ADDRESS, AND ZIP CODE Booz Allen Hamilton 8283 Greensboro Dr. McLean, VA 22102		b. CAGE CODE 17038		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) Chantilly 1 Field Office Email: DSS.Chantilly1@mail.mil Phone: 571-373- 5205			
7. SUBCONTRACTOR							
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)			
8. ACTUAL PERFORMANCE							
a. LOCATION Defense Advanced Research Project Agency (DARPA) 675 N. Randolph St. Arlington, VA 22203		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)			
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT							
Biological Technologies Office - Systems, Engineering and Technical Assistance Support.							
10. CONTRACTOR WILL REQUIRE ACCESS TO:							
YES NO							
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X					
b. RESTRICTED DATA				X			
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION				X			
d. FORMERLY RESTRICTED DATA				X			
e. INTELLIGENCE INFORMATION				X			
(1) Sensitive Compartmented Information (SCI)		X					
(2) Non-SCI		X					
f. SPECIAL ACCESS INFORMATION		X					
g. NATO INFORMATION				X			
h. FOREIGN GOVERNMENT INFORMATION				X			
i. LIMITED DISSEMINATION INFORMATION				X			
j. FOR OFFICIAL USE ONLY INFORMATION		X					
k. OTHER (Specify) *ACCM		X					
11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:							
YES NO							
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X					
b. RECEIVE CLASSIFIED DOCUMENTS ONLY				X			
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		X					
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE				X			
e. PERFORM SERVICES ONLY				X			
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES				X			
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER				X			
h. REQUIRE A COMSEC ACCOUNT				X			
i. HAVE TEMPEST REQUIREMENTS				X			
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X					
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE				X			
l. OTHER (Specify)				X			

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)

No information, except as provided in applicable U.S. Statutes, which is classified of unclassified pertaining to this contract shall be released for public dissemination without prior written approval of DARPA.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Contract # D16PC00068.

8a: The contractor is authorized to work at the following facility up to the Secret/TS level.
(ref. DoDM5220.22-M (2-100a))

10a: Classified COMSEC information/material will be protected IAW DoD 5220.22-M. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. In accordance with DoD5220.22-M (9-407), further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior written approval of the DARPA, Contracting Officer for Security Matters. (ref. DoD 5220.22-M (Ch 9, Sec 4))

10e(1): SCI Access required. The Director, DIA and Director, DARPA, have exclusive security responsibility for SCI released to the contractor or developed under this contract. Before releasing or providing SCI to contractor personnel, the GCA shall ensure that they are appropriately cleared in accordance with ICD 704, and they agree to follow controls and procedures for the protection, handling, and accountability of SCI. All activities involving SCI (including discussions) shall be conducted in sensitive compartmented information facilities (SCIFs). Physical security standards for SCIFs are contained in ICD 705 must be adhered to. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10e(2): Access to Intelligence information is required for performance. The Director, DARPA, has exclusive security responsibility for Non-SCI released to the contractor or developed under this contract. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirement to the cognizant security office. Use Item 13 if additional space is needed.)

Program information shall be protected in accordance with various DARPA and other agency security classification guidance, to be provided by cognizant DARPA PSO(s).

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

SAP: DARPA is responsible for inspection of all SAP materials under this contract.

SCI: DIA is responsible for inspection of all SCI materials under this contract.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
(b)(6)	(b)(6)	(b)(6)
d. ADDRESS (Include Zip Code)	17. REQUIRED DISTRIBUTION	
Defense Advanced Research Project Agency	☒ a. CONTRACTOR	
675 n. Ral	☐ b. SUBCONTRACTOR	
Arlington,	☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR	
e. SIGNA	☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION	
	☒ e. ADMINISTRATIVE CONTRACTING OFFICER	
	☒ f. OTHERS AS NECESSARY	

UNCLASSIFIED

CONTINUATION SHEET FOR DD 254, CONTRACT SECURITY CLASSIFICATION SPECIFICATION

CONTRACT NUMBER
D16PC00068

10f: SAP activities will be accredited, governed, maintained, marked and protected in accordance with DoDM 5205.07-Volumes (1), (3) and (4); and applicable references, and program security classification guides. Access to SAP information requires employees undergo additional personnel security screening and meet the SAP access standards delineated in the applicable DoD directives and policies. SAP inspections and security oversight while in component facilities are under the cognizance of the DARPA SAPCO, as appropriate. The performer is required to submit an accreditation package (Fixed Facility Checklists (FFC) and other applicable documents) and/or System Security Plans (SSP) to the responsible DARPA PS via "DFASTS." Otherwise, contact your PSO for submission instructions.

Effective May 1, 2015 Program Access Request (PAR) packages will be coordinated using the recently approved PAR and PSQ templates. The approved templates can be found at <http://www.dss.mil/isp/templates.html>.

All Special Access Program (SAP) accredited areas must meet the minimum physical and technical security standards outlined in the DoD 5205.07 SAP Manual Volume 3 and its references in Enclosure 1, before receiving, generating, processing, using, or storing SAP classified information, as appropriate to the accreditation. New SAP accredited areas will be inspected by DARPA physical security prior to accreditation. In accordance with DoDM 5205.07-VI (11-1), DARPA PSO review is required prior to release to subcontractors.
(ref. DoDM 5205.07-Volumes (1), (3) and (4))

10j: For Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in DoD Manual 5200.01 Volume 4, DoD Information Security Program.

10k: Alternative Compensatory Control Measures (ACCM) referenced on DARPA-associated contract DD Forms 254 are established, controlled, managed, and administered by non-DARPA Department of Defense (DoD) entities. Access may be provided by DARPA, but all guidance relating to these ACCM procedures and reporting are the responsibility of the establishing DoD entity.

11a: Contractor performance is restricted to another contractor's facility or Government facility. Contractor has NO storage requirement. DARPA or prime contractor will provide security classification guidance for the performance of this contract.

11c: The contractor requires access to classified source data up to and including Top Secret in support of the work effort. Classified material generated in support of this contract shall be classified in accordance with the source material used or DARPA security classification guidance, which will be provided by the DARPA Program Security Officer or the Program Security Representative. Automated information systems must be certified and accredited by the cognizant security agency prior to processing classified information for a DARPA program. All personnel performing Information Assurance (IA)/cybersecurity related duties on DARPA accredited classified information systems shall meet the requirements set forth in DoD Directive 8140.01, "Cyberspace Workforce Management." All classified information received or generated under this contract is the property of the U.S. Government. At the termination or expiration of this contract, DARPA will be contacted for proper disposition instructions.

11j: The contractor must abide by guidance outlined in the DARPA Security Guide, as well as, the DARPA Baseline Agency OPSEC Plan, which will be provided by the PSO or PSR.

All Contractors performing on this contract shall abide by all current and applicable successor governmental guidance. Please contact your FSO, PSO, or PSR if any questions arise pertaining to the availability of these guidance documents.

All Contractors performing on this contract shall abide by the Open Skies Treaty or other U.S. on-site treaty compliance obligations. In doing so, the Contractor may be required to create and execute treaty compliance plans. These plans must be approved by the cognizant Program Security Officer.

Reports of loss, compromise, or suspected compromise shall be provided to the appropriate DARPA Program Security Officer (PSO) within 24 hours of the incident, in addition to the reporting requirements to DSS outlined in the NISPOM.

All of the above security requirements, where applicable, will flow down to any subcontractors and consultants supporting this contract. Copies of all subcontractor DD 254's should be emailed to the DARPA Industrial Security Office, (b)(6)@darpa.mil.

Biological Technologies Office: (b)(6)

UNCLASSIFIED

Designed using Adobe, DARPA/MSO

CONTINUATION SHEET FOR DD 254, CONTRACT SECURITY CLASSIFICATION SPECIFICATION

CONTRACT NUMBER
D16PC00068

SAVANNAH is the DARPA SAP enterprise information system solution and may be deployed for program support. SAVANNAH can be used to extend existing program networks to improve secure information flow between DARPA and performer sites via a "Single Level Connection." An evaluation of performer requirements concerning "Single Level Connections" is required for prudent use of SAVANNAH capabilities. DARPA AO/DAOs and SCAs will provide guidance on Single Level Connection capabilities and the "Connection Approval Package (CAP)."

SAP information systems will require an authorization-to-operate using the Risk Management Framework (RMF) process outlined in the "Joint Special Access Program Implementation Guide (JSIG), dated April 1, 2016" (or successor document).

SAP information systems utilizing Windows as their operating system must utilize the Windows 10 solution. Information regarding the correct Windows 10 version or its successor will be disseminated by the DARPA PSO or your Cybersecurity System Control Assessor (SCA).

Data Transfers: Data transfers will be performed IAW the processes and procedures outlined in the "DARPA Data Transfer SOP," April 11, 2016, Version 1.4 (or most recent version).

Media Encryption: After October 1, 2017, all portable SAP media must be encrypted. Encryption of Data at Rest shall be implemented on SAP IT IAW DoD SAP CIO specified system type deadlines using NSA approved or FIPS 140-2 compliant products.

SAP IT Disposition: The disposition (e.g., sanitization, destruction and release) of SAP IT by contractors will follow the guidelines outlined in "OSD SAPCO, Disposition of DoD Special Access Program Information Technology Devices," July 27, 2017, to include any follow on OSD SAPCO or OSD SAP CIO guidance or directives that supersede this memorandum. DARPA will keep industry partners updated through their PSOs to ensure most current OSD Directives or Instruction flow down.

SAP IT Assessments will be required of DARPA accredited SAP IT systems. Assessments include but are not limited to the SAP IT Census and SAP IT Scorecard. These assessments are critical in ensuring the size, scope, and complexity of our SAP IT systems are properly recorded, managed, and supported.

Additional SAP related security policy documents may be disseminated via the DARPA PSO IAW applicable statutes, Executive orders, cognizant security agency directives, instructions, manuals, regulations, and memorandums. When this documentation is modified, revised, supplemented, changed or reissued, it constitutes implementable security guidance IAW established effective dates. In cases of doubt over the specific provisions, the contractor should consult the PSO and the Contracting Officer before taking any action or expending program-related funds.

Prime Contractors are required to flow down applicable security policy to their sub-contractors as soon as possible, not to exceed 30 calendar days, of receipt of this guidance.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED TOP SECRET b. LEVEL OF SAFEGUARD REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>			3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>		
☒	a. PRIME CONTRACT NUMBER D16PC00067		☒	a. ORIGINAL <i>(Complete date in all cases)</i> DATE (YYYYMMDD) 20160229	
	b. SUBCONTRACT NUMBER			b. REVISED <i>(Supercedes all previous specs)</i>	REVISION NO. DATE (YYYYMMDD)
	c. SOLICITATION OR OTHER NUMBER	DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete Item 5 in all cases)</i> DATE (YYYYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☒ NO If Yes, complete the following:					
Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? ☐ YES ☒ NO If Yes, complete the following:					
In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.					
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>					
a. NAME, ADDRESS, AND ZIP CODE Strategic Analysis, Inc. 4075 Wilson Blvd., Ste 200 Arlington, VA 22203		b. CAGE CODE 44609	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> Alexandria Field Office Email: Crystalcity.IOFCK1@dss.mil Phone: 571-551-7920		
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>		
8. ACTUAL PERFORMANCE					
a. LOCATION Defense Advanced Research Projects Agency (DARPA) 675 N. Randolph St. Arlington, VA 22203		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>		
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Biological Technologies Office - Scientific, Engineering, Administrative and Technical Support					
10. CONTRACTOR WILL REQUIRE ACCESS TO:		YES NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		YES NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		☒ ☐	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		☐ ☒
b. RESTRICTED DATA		☐ ☒	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		☐ ☒
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		☐ ☒	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		☒ ☐
d. FORMERLY RESTRICTED DATA		☐ ☒	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		☐ ☒
e. INTELLIGENCE INFORMATION		☐ ☒	e. PERFORM SERVICES ONLY		☐ ☒
(1) Sensitive Compartmented Information (SCI)		☒ ☐	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		☐ ☒
(2) Non-SCI		☒ ☐	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		☐ ☒
f. SPECIAL ACCESS INFORMATION		☒ ☐	h. REQUIRE A COMSEC ACCOUNT		☐ ☒
g. NATO INFORMATION		☐ ☒	i. HAVE TEMPEST REQUIREMENTS		☐ ☒
h. FOREIGN GOVERNMENT INFORMATION		☐ ☒	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		☒ ☐
i. LIMITED DISSEMINATION INFORMATION		☐ ☒	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		☐ ☒
j. FOR OFFICIAL USE ONLY INFORMATION		☒ ☐	l. OTHER <i>(Specify)</i>		☐ ☒
k. OTHER <i>(Specify)</i> ACCM		☐ ☒			☐ ☒

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)

No information, except as provided in applicable U.S. Statutes, which is classified or unclassified pertaining to this contract shall be released for public dissemination without prior written approval of DARPA.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

10a: Classified COMSEC information/material will be protected IAW DoD 5220.22-M. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. In accordance with DoD 5220.22-M (9-407), further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior written approval of the DARPA, Contracting Officer for Security Matters. (ref. DoD 5220.22-M (Ch 9, Sec 4).

All Contractors performing on this contract shall abide by all current and applicable successor governmental guidance. Please contact your FSO, PSO or PSR if any questions arise pertaining to the availability of these guidance documents."

All Contractors performing on this contract shall abide by the Open Skies Treaty or other U.S. on-site treaty compliance obligations. In doing so, the Contractor may be required to create and execute treaty compliance plans. These plans must be approved by the cognizant Program Security Officer.

Reports of loss, compromise or suspected compromise shall be provided to the appropriate DARPA Program Security Officer (PSO) within 24 hours of the incident, in addition to the reporting requirements to DSS outlined in the NISPOM.

All of the above security requirements, where applicable, will flow down to any subcontractors and consultants supporting this contract. Copies of all subcontractor DD 254's should be emailed to the DARPA Classification Management Office, (b)(6)@darpa.mil.

Biological Technologies Office POCs: (b)(6)

---See Continuation Sheet---

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirement to the cognizant security office. Use Item 13 if additional space is needed.)

When information is controlled by the United States Munitions List (USML), the contractor must abide by the International Traffic Arms Regulation (ITAR) requirements. Program information shall be protected in accordance with various DARPA and other agency security classification guidance, to be provided by cognizant DARPA PSO(s). The Collateral Secret DARPA Secure Wide Area Network (DSWAN) will be operated IAW the attached DARPA/DSS MOU dated June 20, 2013.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

DARPA is responsible for inspection of all SAP materials under this contract. DIA is responsible for inspection of all SCI materials under this contract. IAW the DARPA/DSS MOU dated June 20, 2013 DSWAN is under the security cognizance of DARPA and may include visits from DARPA DSWAN security to validate the secure operating status.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

b. TITLE

c. TELEPHONE (Include Area Code)

d. ADDRESS (Include Zip Code)

Defense Advanced Research Projects Agency (DARPA)
675 North Randolph Street
Arling (b)(6)

e. SI

17. REQUIRED DISTRIBUTION

- ☒ a. CONTRACTOR
☐ b. SUBCONTRACTOR
☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
☒ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
☒ e. ADMINISTRATIVE CONTRACTING OFFICER
☒ f. OTHERS AS NECESSARY

DD F

Designed using Adobe, DARPA/SSO

CONTINUATION SHEET FOR DD 254, CONTRACT SECURITY CLASSIFICATION SPECIFICATION

CONTRACT NUMBER
D16PC00067

Block 13: (Continued)

10e(1): SCI Access required. The Director, DIA and Director, DARPA, have exclusive security responsibility for SCI released to the contractor or developed under this contract. Before releasing or providing SCI to contractor personnel, the GCA shall ensure that they are appropriately cleared in accordance with ICD 704, and they agree to follow controls and procedures for the protection, handling, and accountability of SCI. All activities involving SCI (including discussions) shall be conducted in sensitive compartmented information facilities (SCIFs). Physical security standards for SCIFs are contained in ICD 705 must be adhered to. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10e(2): Access to Intelligence information is required for performance. The Director, DARPA, has exclusive security responsibility for Non-SCI released to the contractor or developed under this contract. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10f: SAP activities will be accredited, governed, maintained, marked and protected in accordance with DoDM 5205.07-Volumes (1), (3) and (4); and applicable references, and program security classification guides. Access to SAP information requires employees undergo additional personnel security screening and meet the SAP access standards delineated in the applicable DoD directives and policies. SAP inspections and security oversight while in component facilities are under the cognizance of the DARPA SAPCO, as appropriate. The performer is required to submit an accreditation package (Fixed Facility Checklists (FFC) and other applicable documents) and/or System Security Plans (SSP) to the responsible DARPA PSO via "DFASTS." Otherwise, contact your PSO for submission instructions.

Effective May 1, 2015 Program Access Request (PAR) packages will be coordinated using the recently approved PAR and PSQ templates. The approved templates can be found at <http://www.dss.mil/isp/templates.html>.

All Special Access Program (SAP) accredited areas must meet the minimum physical and technical security standards outlined in the DoD 5205.07 SAP Manual Volume 3 and its references in Enclosure 1, before receiving, generating, processing, using, or storing SAP classified information, as appropriate to the accreditation. New SAP accredited areas will be inspected by DARPA physical security prior to accreditation. In accordance with DoDM 5205.07-V1 (11-1), DARPA PSO review is required prior to release to subcontractors. (ref. DoDM 5205.07-Volumes (1), (3) and (4)).

10j: For Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in DoD Manual 5200.01 Volume 4, DoD Information Security Program.

10k: Alternative Compensatory Control Measures (ACCM) referenced on DARPA-associated contract DD Forms 254 are established, controlled, managed, and administered by non-DARPA Department of Defense (DoD) entities. Access may be provided by DARPA, but all guidance relating to these ACCM procedures and reporting are the responsibility of the establishing DoD entity.

11c: The contractor requires access to classified source data up to and including Top Secret in support of the work effort. Classified material generated in support of this contract shall be classified in accordance with the source material used or DARPA security classification guidance, which will be provided by the DARPA Program Security Officer or the Program Security Representative. Automated information systems must be certified and accredited by the cognizant security agency prior to processing classified information for a DARPA program. All personnel performing Information Assurance (IA)/cybersecurity related duties on DARPA accredited classified information systems shall meet the requirements set forth in DoD 8570.01-M "Information Assurance Workforce Improvement Program." All classified information received or generated under this contract is the property of the U.S. Government. At the termination or expiration of this contract, DARPA will be contacted for proper disposition instructions. SAP information systems will require an authorization-to-operate using the Risk Management Framework (RMF) process outlined in the "Joint Special Access Program (SAP) Implementation Guide (JSIG)", Revision 3, dated October 9, 2013 (or successor document).

Ref 11j: The contractor must abide by guidance outlined in the DARPA Security Guide, as well as, the DARPA Baseline Agency OPSEC Plan, which will be provided by the PSO or PSR.

UNCLASSIFIED

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED TOP SECRET b. LEVEL OF SAFEGUARD REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)				3. THIS SPECIFICATION IS: (X and complete as applicable)	
☒ a. PRIME CONTRACT NUMBER D16PC00067		☐ b. SUBCONTRACT NUMBER		☐ a. ORIGINAL (Complete date in all cases) DATE (YYYYMMDD) 20161029	
☐ c. SOLICITATION OR OTHER NUMBER		☐ d. DUE DATE (YYYYMMDD)		☒ b. REVISED (Supersedes all previous specs) REVISION NO. 1 DATE (YYYYMMDD) 20171101	
☐ c. SOLICITATION OR OTHER NUMBER		☐ d. DUE DATE (YYYYMMDD)		☐ c. FINAL (Complete Item 5 in all cases) DATE (YYYYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☒ NO If Yes, complete the following: Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? ☐ YES ☒ NO If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.					
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)					
a. NAME, ADDRESS, AND ZIP CODE Strategic Analysis, Inc. 4075 Wilson Blvd, Suite 200 Arlington, VA 22203		b. CAGE CODE 44419		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) Alexandra I Field Office (HOFCS) DSS.AlexandraI@mail.mil 571-551-7920	
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
8. ACTUAL PERFORMANCE					
a. LOCATION Defense Advanced Research Project Agency (DARPA) 675 N. Randolph St Arlington, VA 22203		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Biological Technologies Office - Systems, Engineering and Technical Assistance (SETA) Support.					
10. CONTRACTOR WILL REQUIRE ACCESS TO: YES NO					
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		☒		YES NO	
b. RESTRICTED DATA		☒		YES NO	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		☒		YES NO	
d. FORMERLY RESTRICTED DATA		☒		YES NO	
e. INTELLIGENCE INFORMATION		☒		YES NO	
(1) Sensitive Compartmented Information (SCI)		☒		YES NO	
(2) Non-SCI		☒		YES NO	
f. SPECIAL ACCESS INFORMATION		☒		YES NO	
g. NATO INFORMATION		☒		YES NO	
h. FOREIGN GOVERNMENT INFORMATION		☒		YES NO	
i. LIMITED DISSEMINATION INFORMATION		☒		YES NO	
j. FOR OFFICIAL USE ONLY INFORMATION		☒		YES NO	
k. OTHER (Specify) *ACCM		☒		YES NO	
11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL: YES NO					
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY					
b. RECEIVE CLASSIFIED DOCUMENTS ONLY					
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL					
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE					
e. PERFORM SERVICES ONLY					
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS, AND TRUST TERRITORIES					
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER					
h. REQUIRE A COMSEC ACCOUNT					
i. HAVE TEMPEST REQUIREMENTS					
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS					
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE					
l. OTHER (Specify)					

DD Form 254, DEC 1999

UNCLASSIFIED

D17PC00067 - Attachment 5 Revision 1

Designed using Adobe, DARPA/MSO

UNCLASSIFIED

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)

No information, except as provided in applicable U.S. Statutes, which is classified or unclassified pertaining to this contract shall be released for public dissemination without prior written approval of DARPA.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes to challenge guidance or the classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Contract # D16PC00067.

8a: The contractor is authorized to work at the following facility up to the Secret/TS level.
(ref. DoDM5220.22-M (2-10b))

10a: Classified COMSEC information/material will be protected IAW DoD 5220.22-M. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. In accordance with DoD5220.22-M (9-407), further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior written approval of the DARPA, Contracting Officer for Security Matters. (ref. DoD 5220.22-M (Ch 9, Sec 4))

10c(1): SCI Access required. The Director, DIA and Director, DARPA, have exclusive security responsibility for SCI released to the contractor or developed under this contract. Before releasing or providing SCI to contractor personnel, the GCA shall ensure that they are appropriately cleared in accordance with ICD 704, and they agree to follow controls and procedures for the protection, handling, and accountability of SCI. All activities involving SCI (including discussions) shall be conducted in sensitive compartmented information facilities (SCIFs). Physical security standards for SCIFs are contained in ICD 705 must be adhered to. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

10c(2): Access to Intelligence information is required for performance. The Director, DARPA, has exclusive security responsibility for Non-SCI released to the contractor or developed under this contract. In accordance with DoD5220.22-M (9-304), written concurrence of the DARPA, Contracting Officer for Security Matters is required prior to subcontracting. (ref. DoDM5220.22-M (Ch 9, Sec 3))

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract ☒ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirement to the cognizant security office. Use Item 13 if additional space is needed.)

Program information shall be protected in accordance with various DARPA and other agency security classification guidance, to be provided by cognizant DARPA PSO(s).

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office ☒ Yes ☐ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

SAP: DARPA is responsible for inspection of all SAP materials under this contract.

SCI: DIA is responsible for inspection of all SCI materials under this contract.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL (b)(6)	b. TITLE (b)(6)	c. TELEPHONE (Include Area Code) (b)(6)
d. ADDRESS (Include Zip Code) Defense Advanced Research Projects Agency 675 N. Randolph Street Arlington, VA 22203 (b)(6)		17. REQUIRED DISTRIBUTION ☒ a. CONTRACTOR ☐ b. SUBCONTRACTOR ☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR ☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION ☒ e. ADMINISTRATIVE CONTRACTING OFFICER ☒ f. OTHERS AS NECESSARY
e. SIGNATURE		

DD Form 254 (Back), DEC 1999

UNCLASSIFIED

Designed using Adobe, DARPA/MSO

UNCLASSIFIED

CONTINUATION SHEET FOR DD 254, CONTRACT SECURITY CLASSIFICATION SPECIFICATION

CONTRACT NUMBER
D16PC30067

10f: SAP activities will be accredited, governed, maintained, marked and protected in accordance with DoDM 5205.07-Volumes (1), (3) and (4); and applicable references, and program security classification guides. Access to SAP information requires employees undergo additional personnel security screening and meet the SAP access standards delineated in the applicable DoD directives and policies. SAP inspections and security oversight while in component facilities are under the cognizance of the DARPA SAPCO, as appropriate. The performer is required to submit an accreditation package (Fixed Facility Checklists (FFC) and other applicable documents) and/or System Security Plans (SSP) to the responsible DARPA PS via "DFASTS." Otherwise, contact your PSO for submission instructions.

Effective May 1, 2015 Program Access Request (PAR) packages will be coordinated using the recently approved PAR and PSQ templates. The approved templates can be found at <http://www.dss.mil/isp/templates.html>.

All Special Access Program (SAP) accredited areas must meet the minimum physical and technical security standards outlined in the DoD 5205.07 SAP Manual Volume 3 and its references in Enclosure 1, before receiving, generating, processing, using, or storing SAP classified information, as appropriate to the accreditation. New SAP accredited areas will be inspected by DARPA physical security prior to accreditation. In accordance with DoDM 5205.07-V1 (11-1), DARPA PSO review is required prior to release to subcontractors. (ref. DoDM 5205.07-Volumes (1), (3) and (4))

10j: For Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in DoD Manual 5200.01 Volume 4, DoD Information Security Program.

10k: Alternative Compensatory Control Measures (ACCM) referenced on DARPA-associated contract DD Forms 254 are established, controlled, managed, and administered by non-DARPA Department of Defense (DoD) entities. Access may be provided by DARPA, but all guidance relating to these ACCM procedures and reporting are the responsibility of the establishing DoD entity.

11a: Contractor performance is restricted to another contractor's facility or Government facility. Contractor has NO storage requirement. DARPA or prime contractor will provide security classification guidance for the performance of this contract.

11c: The contractor requires access to classified source data up to and including Top Secret in support of the work effort. Classified material generated in support of this contract shall be classified in accordance with the source material used or DARPA security classification guidance, which will be provided by the DARPA Program Security Officer or the Program Security Representative. Automated information systems must be certified and accredited by the cognizant security agency prior to processing classified information for a DARPA program. All personnel performing Information Assurance (IA)/cybersecurity-related duties on DARPA accredited classified information systems shall meet the requirements set forth in DoD Directive R140.01, "Cyberspace Workforce Management." All classified information received or generated under this contract is the property of the U.S. Government. At the termination or expiration of this contract, DARPA will be contacted for proper disposition instructions.

11j: The contractor must abide by guidance outlined in the DARPA Security Guide, as well as, the DARPA Baseline Agency OPSEC Plan, which will be provided by the PSO or PSR.

All Contractors performing on this contract shall abide by all current and applicable successor governmental guidance. Please contact your FSO, PSO, or PSR if any questions arise pertaining to the availability of these guidance documents.

All Contractors performing on this contract shall abide by the Open Skies Treaty or other U.S. on-site treaty compliance obligations. In doing so, the Contractor may be required to create and execute treaty compliance plans. These plans must be approved by the cognizant Program Security Officer.

Reports of loss, compromise, or suspected compromise shall be provided to the appropriate DARPA Program Security Officer (PSO) within 24 hours of the incident, in addition to the reporting requirements to DSS outlined in the NISPOM.

All of the above security requirements, where applicable, will flow down to any subcontractors and consultants supporting this contract. Copies of all subcontractor DD 254's should be emailed to the DARPA Industrial Security Office (b)(6)@darpa.mil.

Biological Technologies Office: (b)(6)

UNCLASSIFIED

Designed using Adobe, DARPA/MSO

UNCLASSIFIED

CONTINUATION SHEET FOR DD 254, CONTRACT SECURITY CLASSIFICATION SPECIFICATION

CONTRACT NUMBER
D16PC00067

SAVANNAH is the DARPA SAP enterprise information system solution and may be deployed for program support. SAVANNAH can be used to extend existing program networks to improve secure information flow between DARPA and performer sites via a "Single Level Connection." An evaluation of performer requirements concerning "Single Level Connections" is required for prudent use of SAVANNAH capabilities. DARPA AO/DAOs and SCAs will provide guidance on Single Level Connection capabilities and the "Connection Approval Package (CAP)."

SAP information systems will require an authorization-to-operate using the Risk Management Framework (RMF) process outlined in the "Joint Special Access Program Implementation Guide (JSIG), dated April 1, 2016" (or successor document).

SAP information systems utilizing Windows as their operating system must utilize the Windows 10 solution. Information regarding the correct Windows 10 version or its successor will be disseminated by the DARPA PSO or your Cybersecurity System Control Assessor (SCA).

Data Transfers: Data transfers will be performed IAW the processes and procedures outlined in the "DARPA Data Transfer SOP," April 11, 2016, Version 1.4 (or most recent version).

Media Encryption: After October 1, 2017, all portable SAP media must be encrypted. Encryption of Data at Rest shall be implemented on SAP IT IAW DoD SAP CIO specified system type deadlines using NSA approved or FIPS 140-2 compliant products.

SAP IT Disposition: The disposition (e.g., sanitization, destruction and release) of SAP IT by contractors will follow the guidelines outlined in "OSD SAPCO, Disposition of DoD Special Access Program Information Technology Devices," July 27, 2017, to include any follow on OSD SAPCO or OSD SAP CIO guidance or directives that supersede this memorandum. DARPA will keep industry partners updated through their PSOs to ensure most current OSD Directives or Instruction flow down.

SAP IT Assessments will be required of DARPA accredited SAP IT systems. Assessments include but are not limited to the SAP IT Census and SAP IT Scorecard. These assessments are critical in ensuring the size, scope, and complexity of our SAP IT systems are properly recorded, managed, and supported.

Additional SAP related security policy documents may be disseminated via the DARPA PSO IAW applicable statutes, Executive orders, cognizant security agency directives, instructions, manuals, regulations, and memorandums. When this documentation is modified, revised, supplemented, changed or reissued, it constitutes implementable security guidance IAW established effective dates. In cases of doubt over the specific provisions, the contractor should consult the PSO and the Contracting Officer before taking any action or expending program-related funds.

Prime Contractors are required to flow down applicable security policy to their sub-contractors as soon as possible, not to exceed 30 calendar days, of receipt of this guidance.

UNCLASSIFIED

Designed using Adobe, DARPA/MSO



RESOLUCIÓN DE DIRECCION GENERAL
N° 028 -2017-SERFOR/DGGSPFFS

Lima, **01 FEB. 2017**

VISTO:

La solicitud presentada el 21 de diciembre de 2016 por el señor William Valderrama Bazán y el Informe Técnico N° 068-2017-SERFOR/DGGSPFFS-DGSPFS de fecha 30 de enero de 2017;

CONSIDERANDO:

Que, el artículo 4° de la Ley N° 27444, establece los principios del procedimiento administrativo, los cuales refieren que los administrados gozan de todos los derechos y garantías inherentes al debido procedimiento administrativo;

Que, el numeral 2° de la normativa antes mencionada, indica que los principios del procedimiento administrativo, servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las reglas de procedimiento, como parámetros para la generación de otras disposiciones administrativas de carácter general, y para suplir los vacíos en el ordenamiento administrativo;

Que, mediante el Decreto Supremo N° 007-2013-MINAGRI, modificado por el Decreto Supremo N° 016-2014-MINAGRI, se aprobó el Reglamento de Organización y Funciones - ROF del Servicio Nacional Forestal y de Fauna Silvestre - SERFOR, el mismo que en su literal "g" del artículo 53°, señala como una de las funciones de la Dirección General de Gestión Sostenible del Patrimonio Forestal y de Fauna Silvestre, la de otorgar permisos de investigación o de difusión cultural con o sin colecta de flora y fauna silvestre y sus recursos genéticos;

Que, mediante Resolución de Dirección General N° 040-2016-SERFOR-DGGSPFFS, de fecha 20 de enero de 2016, se autorizó al señor William Valderrama Bazán realizar investigación científica de fauna silvestre con colecta de especímenes para el proyecto "Evaluación de la vacunación de murciélagos hematófagos (*Desmodus rotundus*) para el control de la rabia bovina en Apurímac", a realizarse en las provincias de Antabamba, Aymaraes, Cotabambas y Grau, departamento de Apurímac por el periodo de hasta dos (02) años;

Que, mediante Carta N° 025-2016-RENACE recibida el 21.12.2016 con CUT N° 48105-2016, suscrita por el señor William Valderrama Bazán, responsable del proyecto "Evaluación de la vacunación de murciélagos hematófagos (*Desmodus rotundus*) para el control de la rabia bovina en Apurímac", solicita la modificación de la R.D.G. N° 040-2016-SERFOR-DGGSPFFS (20.01.2016), respecto a la inclusión de estudios con biomarcadores y la colecta de pelos en tres (03) colonias de murciélagos hematófagos (*Desmodus rotundus*) en el departamento de Lima y la ampliación del cronograma del estudio;

Que, el informe técnico del visto, concluye entre otros que el señor William Valderrama Bazán, ha cumplido con presentar la información que justifica la modificación de la R.D.G. N° 040-2016-SERFOR-DGGSPFFS de fecha 20 de enero de 2016; asimismo recomienda que, por las razones técnicas señaladas en el referente informe, se otorgue lo solicitado por el señor William Valderrama Bazán;



En uso de las atribuciones conferidas por el artículo 53° del Reglamento de Organización y Funciones del Servicio Nacional Forestal y de Fauna Silvestre-SERFOR, aprobado por Decreto Supremo N° 007-2013-MINAGRI, el mismo que en su literal "g" del mencionado artículo señala como una de las funciones de la Dirección General de Gestión Sostenible del Patrimonio Forestal y de Fauna Silvestre, la de otorgar permisos de investigación con o sin colecta de flora y fauna silvestre y sus recursos genéticos.

SE RESUELVE:

Artículo 1°.- Modificar la R.D.G. N° 040-2016-SERFOR-DGGSPFFS de fecha 20.01.2016, en su Artículo 1°, incluyendo los estudios con los biomarcadores DayGlo y Rodomina B, la colecta de hasta 2400 muestras de pelos provenientes de tres (03) colonias de murciélagos de la especie *Desmodus rotundus*, la inclusión de localidades de estudio en los distritos de Paramonga, Huacho y Pachacamac en el departamento de Lima y la ampliación del cronograma del estudio hasta por seis meses adicionales.

Artículo 2°.- Mantener vigente en todos sus extremos los demás textos de la R.D.G. N° 040-2016-SERFOR-DGGSPFFS (20.01.2016).

Artículo 3°.- Notificar la presente Resolución al señor William Valderrama Bazán y transcribirla a la Dirección General de Información y Ordenamiento Forestal y de Fauna Silvestre y a las Administraciones Técnicas Forestales y de Fauna Silvestre de Apurímac y Lima para su conocimiento, seguimiento y/o verificación de ejecución.

Artículo 4°.- Disponer la publicación de la presente Resolución en el Portal Web del Servicio Nacional Forestal y de Fauna Silvestre: www.serfor.gob.pe.



Regístrese y comuníquese

Ing. Walter Nalvarte Armas
Director General
Dirección General de Gestión Sostenible del
Patrimonio Forestal y de Fauna Silvestre
Servicio Nacional Forestal y de Fauna Silvestre - SERFOR



RESOLUCIÓN DE DIRECCION GENERAL
N° 054 -2016-SERFOR/DGGSPFFS

Lima, 28 ENE 2016

VISTO:

El Informe Técnico N° 0081-2016-SERFOR/DGGSPFFS-DGSPFS, de fecha 26 de enero del 2016, y;

CONSIDERANDO:

Que, mediante Carta N° IBAHCMPE2015-01, presentada el 22 de abril del 2015, el Doctor Daniel Gregory Streicker, investigador del Instituto de Biodiversidad, Salud Animal y Medicina Comparativa de la Universidad Glasgow, Reino Unido, solicitó la Inscripción previa en el Registro Público de Acceso a Recursos Genéticos y Subscripción de Contrato de Acceso Marco para el desarrollo del Proyecto de Investigación Titulado: "Caracterización, distribución y ecología de enfermedades infecciosas en el vampiro común (*Desmodus rotundus*)";

Que, el artículo 140 de la Ley N° 29763, Ley Forestal y de Fauna Silvestre, indica que: "La colecta o extracción de recursos forestales y de fauna silvestre con fines de investigación, orientada a la determinación de genotipo, filogenia, sistemática y biogeografía es autorizada siguiendo procedimientos simplificados establecidos por el SERFOR. Los requisitos y procedimientos para la colecta o extracción y la exportación de especímenes de flora y fauna silvestre con fines de investigación o propósito cultural lo establece el reglamento de la presente Ley, teniendo en cuenta las normas específicas relacionadas;

Que, mediante Decreto Supremo N° 019-2015-MINAGRI, se aprobó el Reglamento para la Gestión de la Fauna Silvestre de la Ley N° 29763, Ley Forestal y de Fauna Silvestre;

Que, el artículo 134.5 del Decreto Supremo N° 019-2015-MINAGRI, establece que el desarrollo de actividades de investigación básica taxonómica de fauna silvestre, relacionada con estudios moleculares con fines taxonómicos, sistemáticos, filogeográficos, biogeográficos, evolutivos y de genética de la conservación, entre otras investigaciones sin fines comerciales, son aprobadas mediante autorizaciones de investigación científica;

Que, mediante Resolución de Dirección Ejecutiva N° 031-2014-SERFOR-DE, emitida por el Servicio Nacional Forestal y de Fauna Silvestre – SERFOR, se encargó al Blgo. Mirbel Alberto Epiquián Rivera las funciones de Director General de Gestión Sostenible del Patrimonio Forestal y de Fauna Silvestre del Servicio Nacional Forestal y de Fauna Silvestre – SERFOR;



Que, el Informe Técnico N° 0081-2016-SERFOR/DGGSPFFS-DGSPFS, de fecha 26 de enero del 2016, emitido por la Dirección de Gestión Sostenible del Patrimonio Fauna Silvestre, señala que el proyecto titulado: "Caracterización, distribución y ecología de enfermedades infecciosas en el vampiro común (*Desmodus rotundus*)", se realizará con muestras biológicas que fueron colectadas al amparo de las autorizaciones: N° 103-2008-INRENA-IFFS-DCB, RD N° 222-2009-AG-DGFFS-DGEFFS, RD N° 0299-2010-AG-DGFFS-DGEFFS, RD 273-2012-AG-DGFFS-DGEFFS y RDG N° 0142-2015-SERFOR/DGGSPFFS; e involucra análisis moleculares, los cuales incluyen, entre otros, extracción, amplificación y secuenciamiento de ADN mitocondrial y nuclear, amplificación y genotipificación de microsatélites, extracción de ácidos nucleicos virales y análisis metagenómico; con la finalidad de realizar estudios de genética poblacional en colonias del murciélago de la especie *Desmodus rotundus*, determinar la diversidad de las fuentes de alimentación en ésta especie y detectar la circulación de virus de importancia en salud pública. Es decir, éstas técnicas moleculares involucran el uso del material genético contenido en los recursos biológicos, con el propósito de realizar estudios de análisis genético, los cuales no tienen fines comerciales, según lo observado en la solicitud;

Que, el precitado Informe señala que el Decreto Supremo N° 019-2015-MINAGRI, "Reglamento para la Gestión de Fauna Silvestre", aprobado el 30 de setiembre del 2015, establece que las investigaciones que usan herramientas moleculares con fines taxonómicos u otros relacionados son aprobadas mediante autorización de investigación científica, y;

En uso de las atribuciones conferidas por el artículo 53° del Reglamento de Organización y Funciones del Servicio Nacional Forestal y de Fauna Silvestre-SERFOR, aprobado por Decreto Supremo N° 007-2013-MINAGRI, el mismo que en su literal "g" del mencionado artículo señala como una de las funciones de la Dirección General de Gestión Sostenible del Patrimonio Forestal y de Fauna Silvestre, la de otorgar permisos de investigación o de difusión cultural con o sin colecta de flora y fauna silvestre y sus recursos genéticos.

SE RESUELVE:

Artículo 1°.- Autorizar al Doctor Daniel Gregory Streicker, identificado con PAS N° 488648942, investigador del Instituto de Biodiversidad, Salud Animal y Medicina Comparativa de la Universidad Glasgow, Reino Unido, y su colaboradora, Dra. Laura Michelle Bergner, identificada con PAS N° 483460019, el uso para análisis molecular de las muestras biológicas de *Desmodus rotundus*: biopsia de ala, sangre entera, contenido estomacal y heces fecales; colectadas bajo el amparo de las autorizaciones: N° 103-2008-INRENA-IFFS-DCB, RD N° 222-2009-AG-DGFFS-DGEFFS, RD N° 0299-2010-AG-DGFFS-DGEFFS, RD 273-2012-AG-DGFFS-DGEFFS y RDG N° 0142-2015-SERFOR/DGGSPFFS, para el desarrollo del proyecto titulado: "Caracterización, distribución y ecología de enfermedades infecciosas en el vampiro común (*Desmodus rotundus*)", por un período de cuatro (04) años; contados a partir de la emisión de la presente resolución.





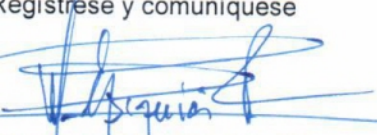
Artículo 2º.- Indicar a los titulares de la presente autorización que, para la exportación de las muestras biológicas que forman parte del proyecto anteriormente citado, deberán solicitar los respectivos permisos de exportación emitidos por el SERFOR, cumpliendo con los requisitos exigidos en los numerales 30 y 31 del Anexo N° 2, del D.S. N° 019-2015-MINAGRI.

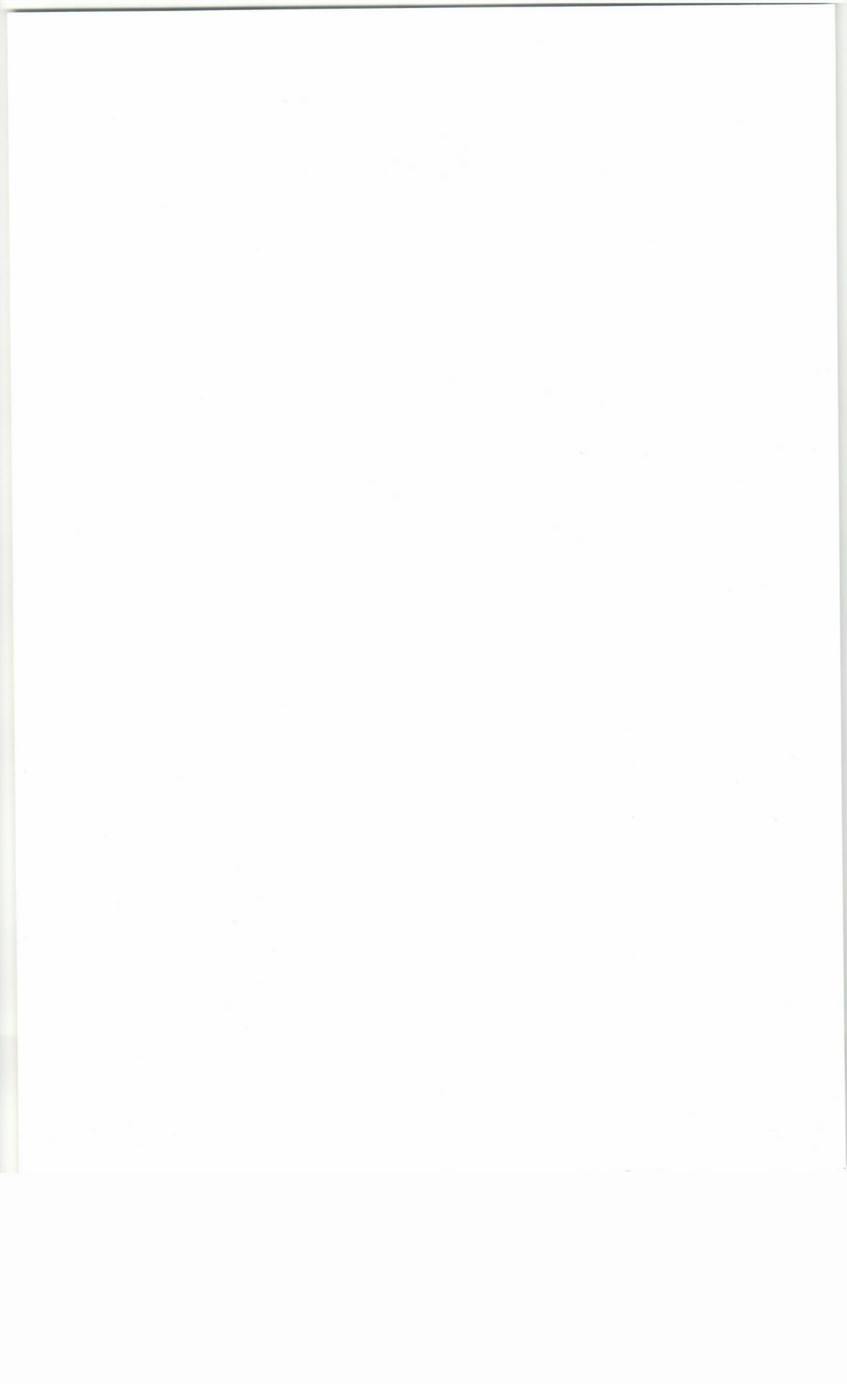
Artículo 3º.- Notificar la presente Resolución de Dirección General al Doctor Daniel Gregory Streicker y transcribirla a la Dirección General de Información y Ordenamiento Forestal y de Fauna Silvestre del SERFOR.

Artículo 4º.- Disponer la publicación de la presente Resolución en el Portal Web del Servicio Nacional Forestal y de Fauna Silvestre: www.serfor.gob.pe.

Regístrese y comuníquese




Blgo. Mirbel Alberto Epiquién Rivera
Director General
Dirección General de Gestión Sostenible del
Patrimonio Forestal y de Fauna Silvestre
Servicio Nacional Forestal y de Fauna Silvestre - SERFOR





RESOLUCIÓN DE DIRECCION GENERAL
Nº 0142 -2015-SERFOR/DGGSPFFS

Lima, 04 JUN. 2015

VISTA:

La solicitud presentada el 27 de marzo del 2015, por el Doctor Daniel Gregory Streicker, investigador del Instituto de Biodiversidad, Salud Animal y Medicina Comparativa de la Universidad Glasgow, Reino Unido, quien solicitó autorización para realizar investigación científica y colecta de fauna silvestre, fuera de Áreas Naturales Protegidas, en el distrito de Imaza, provincia de Bagua, distrito de Chirimoto, provincia de Rodríguez de Mendoza, departamento de Amazonas, distritos de Abancay y Lambrama, provincia de Abancay, distrito de Pacucho, provincia de Andahuaylas, distrito de Tapayrihua, provincia de Aymaraes, distritos de Ahuayro y Rio Blanco, provincia de Chincheros, departamento de Apurímac, distritos de Chungui y San Miguel, provincia de La Mar, y distrito de Ocos, provincia de Vilcashuamán, departamento de Ayacucho, distrito de Chota, provincia de Chota, distritos de Ambulco y Rodeopampa, provincia de Cutervo y distrito de San Ignacio, provincia de Jaén, departamento de Cajamarca; distrito de Limatambo, provincia de Anta, departamento de Cusco; distrito de Cayna, provincia de Ambo, distrito de Molinopampa, provincia de Huánuco, y distritos de Aucayacu y Tingo María, provincia de Tingo María, departamento de Huánuco; distrito de Barranca, provincia de Barranca, distrito de Mala, provincia de Cañete y distritos de Huacho y Chancay, provincia de Huaral, departamento de Lima; distrito de Huepetuhe, provincia de Manu, departamento de Madre de Dios; distrito de Curimana, provincia de Curimana, y distrito de Padre Abad, provincia de Padre Abad, departamento de Ucayali, como parte del estudio titulado "Caracterización, distribución y ecología de enfermedades infecciosas en el vampiro común (*Desmodus rotundus*)"; y,



CONSIDERANDO:

Que, el artículo 66° de la Constitución Política del Perú, establece que los recursos naturales, renovables y no renovables, son patrimonio de la Nación. El Estado es soberano en su aprovechamiento; asimismo, en su artículo 68° establece que es obligación del Estado promover la conservación de la diversidad biológica;

Que, la Ley Nº 26821, Ley Orgánica para el Aprovechamiento Sostenible de los Recursos Naturales, establece en su artículo 9°, referido a la investigación científica, que el Estado promueve la investigación científica y tecnológica sobre la diversidad, calidad, composición, potencialidad y gestión de los recursos naturales. Asimismo, promueve la información y el conocimiento sobre los recursos naturales. Para estos efectos, podrán otorgarse permisos para investigación en materia de recursos naturales;

Que, el Reglamento de la Ley Forestal y de Fauna Silvestre, aprobado por el Decreto Supremo Nº 014-2001-AG, establece en su artículo 328° que la investigación científica o estudio que implique colección de especímenes o elementos de la flora y fauna silvestre no vedados y la obtención de datos e información de campo, requiere autorización del INRENA;

Que, mediante Decreto Legislativo N° 997, Decreto Legislativo que aprueba la Ley de Organización y Funciones del Ministerio de Agricultura, ahora Ministerio de Agricultura y Riego, modificado por la Ley N° 30048, dispone que este Ministerio es el órgano rector del Sector Agrario, el cual comprende entre otras: las tierras de uso agrícola, de pastoreo, las tierras forestales, las eriazas con aptitud agraria; los recursos forestales y su aprovechamiento; la flora y fauna; las actividades de producción, transformación y de comercialización de cultivos y crías; asimismo, dispone, entre otros, que este Ministerio diseña, establece, ejecuta y supervisa las políticas nacionales y sectoriales en materia agraria; ejerce la rectoría en relación con ella y vigila su obligatorio cumplimiento por los tres niveles de gobierno;

Que, el artículo 13 de la Ley N° 29763, crea el Servicio Nacional Forestal y de Fauna Silvestre-SERFOR, como organismo público técnico especializado, con personería jurídica de derecho público interno, como pliego presupuestal adscrito al Ministerio de Agricultura y Riego. Asimismo, se señala que el SERFOR es la autoridad nacional forestal y de fauna silvestre, ente rector del Sistema Nacional de Gestión Forestal y de Fauna Silvestre (SINAFOR), y se constituye en su autoridad técnico normativa a nivel nacional, encargada de dictar las normas y establecer los procedimientos relacionados a su ámbito;

Que, mediante Decreto Supremo N° 007-2013-MINAGRI, se aprobó el Reglamento de Organización y Funciones - ROF del Servicio Nacional Forestal y de Fauna Silvestre - SERFOR, el mismo que en su literal g) del artículo 53°, señala como una de las funciones de la Dirección General de Gestión Sostenible del Patrimonio Forestal y de Fauna Silvestre, la de otorgar permisos de investigación o de difusión cultural con o sin colecta de flora y fauna silvestre y sus recursos genéticos;

Que, mediante Decreto Supremo N° 016-2014-MINAGRI, se aprobó la modificación del Reglamento de Organización y Funciones del Servicio Nacional Forestal y de Fauna Silvestre – SERFOR, aprobado con Decreto Supremo N° 007-2013-MINAGRI;

Que, mediante Resolución Ministerial N° 424-2014-MINAGRI, se da por concluido el proceso de transferencia de la Dirección General Forestal y de Fauna Silvestre al Servicio Nacional Forestal y de Fauna Silvestre – SERFOR, así como el proceso de fusión por absorción, entre otros;

Que, la Tercera Disposición Final del Reglamento de Acceso a los Recursos Genéticos, aprobado por Resolución Ministerial N° 087-2008-MINAM, señala que la obtención de permisos, autorizaciones y demás documentos que otorguen entidades públicas, tales como el Ministerio de Agricultura y que amparen la investigación, obtención, provisión, transferencia u otro de recursos biológicos, con fines distintos a su utilización como fuente de recursos genéticos, no faculta a sus titulares a utilizar dichos recursos como medio para acceder a los recursos genéticos, ni determinan ni presumen autorización de acceso;

Que, mediante el Decreto Supremo N° 003-2009-MINAM que eleva a rango de Decreto Supremo la Resolución Ministerial N° 087-2008-MINAM, y ratifica la aprobación del Reglamento de Acceso a Recursos Genéticos efectuadas por la referida Resolución;





Que, el Decreto Supremo N° 004-2014-MINAGRI, aprueba la actualización de la lista de clasificación y categorización de las especies amenazadas de fauna silvestre legalmente protegidas;

Que, mediante Resolución Ministerial N° 212-2011-AG, se aprueba la modificación al Texto Único de Procedimientos Administrativos (TUPA) del Ministerio de Agricultura y Riego, el mismo que establece en su procedimiento 21, los requisitos de la autorización para realizar actividades de investigación científica y filmaciones con fines comerciales de flora y fauna fuera de Áreas Naturales Protegidas, el mismo que resulta aplicable para el presente procedimiento, en virtud de lo dispuesto en el artículo 6° de la Resolución Ministerial N° 0424-2014-MINAGRI;

Que, mediante Resolución de Dirección Ejecutiva N° 031-2014-SERFOR-DE, emitida por el Servicio Nacional Forestal y de Fauna Silvestre – SERFOR, se encargó al Blgo. Mirbel Alberto Epiquián Rivera las funciones de Director General de Gestión Sostenible del Patrimonio Forestal y de Fauna Silvestre del Servicio Nacional Forestal y de Fauna Silvestre – SERFOR;

Que, el Informe N° 613-2015-SERFOR/DGGSPFFS-DGSPFS, de fecha 21 de mayo del 2015, emitido por la Dirección de Gestión Sostenible del Patrimonio Fauna Silvestre, señala que la presente investigación reviste de importancia debido a que contribuirá al conocimiento relacionado a la transmisión de enfermedades infecciosas en *Desmodus rotundus*, especialmente en los mecanismos de transmisión y difusión espacial de la rabia con fines de mejorar programas de prevención y control de la rabia silvestre en seres humanos y animales domésticos;

Que, el precitado Informe señala que la solicitud materia de resolución, cumple con los requisitos establecidos por el Texto Único de Procedimientos Administrativos del Ministerio de Agricultura y Riego; y,

En uso de las atribuciones conferidas por el artículo 53° del Reglamento de Organización y Funciones del Servicio Nacional Forestal y de Fauna Silvestre-SERFOR, aprobado por Decreto Supremo N° 007-2013-MINAGRI, el mismo que en su literal "g" del mencionado artículo señala como una de las funciones de la Dirección General de Gestión Sostenible del Patrimonio Forestal y de Fauna Silvestre, la de otorgar permisos de investigación o de difusión cultural con o sin colecta de flora y fauna silvestre y sus recursos genéticos.

SE RESUELVE:

Artículo 1°.- Autorizar al Dr. Daniel Gregory Streicker, realizar la investigación científica en fauna silvestre, fuera de Áreas Naturales Protegidas, con captura temporal de murciélagos *Desmodus rotundus* y especies de los siguientes géneros: *Artibeus*, *Carollia*, *Glossophaga*, *Myotis* y otros géneros asociados (no CITES), para la colecta del siguiente tipo de muestras: sangre entera, frotices y suero sanguíneos, pelo, contenido estomacal, biopsia de ala, hisopados orales y rectales, heces, orina y ectoparásitos, así como colecta definitiva de no más de un mil y doscientos (1200) individuos de *Desmodus rotundus* para muestras de: cerebro, glándulas salivales, riñones, hígado, pulmones y bazo; solicitada como parte del proyecto titulado "Caracterización, distribución y ecología de enfermedades infecciosas en el vampiro común (*Desmodus rotundus*)", a ser realizado en los departamentos de Amazonas, Apurímac, Ayacucho, Cajamarca, Cusco, Huánuco, Lima, Madre de Dios y Ucayali; por el periodo de cuatro (04) años, contados a partir de la emisión de la presente resolución, en el cual participarán los siguientes investigadores:



NOMBRE	NACIONALIDAD	DOCUMENTO	N°
DANIEL GREGORY STREICKER	Estadounidense	PAS	018292192
CARLOS EDUARDO TELLO CHINININ	Peruana	DNI	40317512
JULIO ANDRE BENAVIDES TALA	Chilena	PAS	P03409393
LAURA MICHELLE BERGNER	Estadounidense	PAS	483460019
NÉSTOR GERARDO FALCÓN PÉREZ	Peruana	DNI	08679280
CARLOS MARTÍN SHIVA RAMAYONI	Peruana	DNI	21859605

Artículo 2°.- El titular de la autorización y los investigadores señalados en el artículo precedente se comprometen a:

- Colectar únicamente los especímenes autorizados.
- No ceder el material colectado a terceros.
- Comunicar la entrada y salida del personal científico en campo a la Administración Técnica Forestal y de Fauna Silvestre (ATFFS) o la Autoridad en materia forestal y de fauna silvestre del Gobierno Regional de la jurisdicción en donde se llevará a cabo el proyecto, así como informar brevemente sobre el tipo y cantidad de muestras colectadas.
- Si por razones científicas acotadas, se requiere enviar al extranjero parte del material colectado, los interesados deberán gestionar el correspondiente Permiso de Exportación ante la Dirección General de Gestión Sostenible del Patrimonio Forestal y de Fauna Silvestre del SERFOR, así como pasar el control respectivo.
- Entregar el 50% del material colectado por especie y tipo de muestra a una institución científica nacional debidamente reconocida. Los ejemplares únicos de los grupos taxonómicos colectados y holotipos, solo podrán ser exportados en calidad de préstamo.
- No contactar, ni ingresar a los territorios comunales sin contar con la autorización de las autoridades comunales correspondientes.
- Entregar a la Dirección General de Gestión Sostenible del Patrimonio Forestal y de Fauna Silvestre una (01) copia del informe parcial, al término de cada año del otorgamiento de la presente autorización.
- Entregar a la Dirección General de Gestión Sostenible del Patrimonio Forestal y de Fauna Silvestre una (01) copia del informe final en idioma español, como resultado de la autorización otorgada, copias del material fotográfico y/o slides que puedan ser utilizadas para difusión. Asimismo, entregar una (01) copia de las publicaciones, producto de la investigación realizada en formato impreso y digital, que incluya la lista taxonómica de las especies de fauna y flora objeto de la presente autorización de colecta con las respectivas coordenadas (en formato excel).
- La entrega de lo indicado en los literales e) y h), no deberá tomar un plazo mayor a los seis (06) meses al vencimiento de la presente autorización.
- Indicar el número de la Resolución en las publicaciones generadas a partir de la autorización concedida.

Artículo 3°.- La Dirección General de Gestión Sostenible del Patrimonio Forestal y de Fauna Silvestre no se responsabiliza por accidentes o daños sufridos por la solicitante y los investigadores mencionado en el artículo 1°, durante la ejecución del proyecto; asimismo, se reserva el derecho de demandar del proyecto de investigación los cambios a que hubiese lugar en los casos en que se dicten nuevas disposiciones legales o se formulen ajustes sobre la presente autorización.



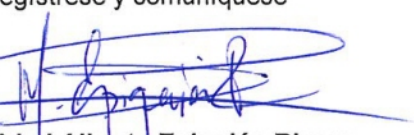


Artículo 4º.- Los derechos otorgados sobre los recursos biológicos no otorgan derechos sobre los recursos genéticos contenidos en ellos, ni autorizan el estudio a nivel genético, de acuerdo con la Tercera Disposición Final del Reglamento de Acceso a los Recursos Genéticos, aprobado por Resolución Ministerial 087-2008-MINAM, y elevado al Rango de Decreto Supremo mediante Decreto Supremo N° 003-2009-MINAM.

Artículo 5º.- Notificar la presente Resolución al Doctor Daniel Gregory Streicker y transcribirla a la Dirección General de Información y Ordenamiento Forestal y de Fauna Silvestre del SERFOR, a las Administraciones Técnicas Forestales y de Fauna Silvestre de Apurímac, Cajamarca, Cusco y Lima, a la Dirección Ejecutiva de Gestión de Bosques y Fauna Silvestre de la Autoridad Regional Ambiental del Gobierno Regional de Amazonas, a la Dirección del Ambiente y Recursos Naturales del Gobierno Regional de Ayacucho, a la Dirección Regional de Agricultura del Gobierno Regional de Huánuco, a la Dirección Regional Forestal y de Fauna Silvestre del Gobierno Regional de Madre de Dios y a la Dirección Ejecutiva Forestal y de Fauna Silvestre del Gobierno Regional de Ucayali.

Regístrese y comuníquese




Blgo. Mirbel Alberto Epiquién Rivera
Director General
Dirección General de Gestión Sostenible del
Patrimonio Forestal y de Fauna Silvestre

