Aircraft/UAV Checklist

[Insert Org Name]

[Date]

[Address]

This page intentionally left blank.

CHECK Applicable blocks		
☐ Initial Accreditation	☐ Re- Accreditation	☐ Modified Facility
☐ Pre-construction	☐ New Facility	☐ Page Change

Checklist Contents

Section A: **General information**

Section B: **Physical Security**

Section C: **Intrusion Detection Systems (IDS)**

Section D: **Classified Destruction Methods**

Section E: **TEMPEST/Technical Security**

List of Attachments

(Diagrams must be submitted on 8 ½'' x 11'' or 11'' x 17'' format)

		Section A: General Information		
1.	**SCIF Data**			
		a. Organization/ Company Name		
		b. Type of Aircraft and Tail Number		
		c. Home Station		
		d. SCIF ID Number		
		e. Contract Number and Expiration Date *(if applicable)*		
		f. Concept Approval Date		
		g. Cognizant Security Authority (CSA)		
		h. Defense Special Security Communication System Information *(if applicable)*		
		DSSCS Message Address		
		DSSCS INFO Address		
		If no DSSCS Message Address, please provide passing instructions		
2.	**Complete Mailing Address**			
3.	**E-Mail Address**			
	Classified		(Network/ System Name & Level)	
	Unclassified		(Network/ System Name)	
	Additional		(Network/ System Name)	
4.	**Responsible Security Personnel**			

	PRIMARY	**ALTERNATE**
Name		
Commercial Telephone		
DSN Telephone		
Secure Telephone		
STE Telephone		
Other Telephone		
Home Telephone *(Optional)*		
FAX # Classified		Unclassified

	Command or Regional Special Security Office/Name (SSO): *(if applicable)*		
	Commercial		
	Other Telephone		
		PRIMARY	**ALTERNATE**
	Information System Security Officer Name:		
	Commercial		
	Secure		

5.	**Accreditation Data**						
	a. Category/Compartments of SCI Requested:						
	b. Existing Accreditation Information *(if applicable)*						
	(1) Category/ Compartments of SCI:						
	(2) Accreditation granted by:			On:			
	(3) Co-Use Agreements	☐ Yes	☐ No	If yes, provide sponsor/ compartment:			
	c. Is there a SAP(s) co-located within the aircraft?				☐ Yes		☐ No
	SAP Classification Level *(check all that apply)*						
	☐ SCI	☐ Top Secret		☐ Secret		☐ Confidential	
	d. Has CSA requested any waivers?	☐ Yes	☐ No	☐ N/ A	If yes, attach a copy of the approved waiver		
	Construction/Modification						
	Is construction or modification complete?	☐ Yes	☐ No	☐ N/ A	If no, enter the expected date of completion		

6.	**Inspections**				
	a. Last physical security inspection performed by			On _____ *(Attach a copy of report)*	
	Were deficiencies corrected?	☐ Yes	☐ No	☐ N/ A	If no, explain
	REMARKS:				

Section B: Physical Security

1.	**Stationary Aircraft/UAV**

	a. Is the aircraft located within a controlled area?		☐ Yes	☐ No	☐ N/ A
	If no, explain:				
	b. When not performing a SCI mission is all SCI removed from the aircraft and stored in an accredited SCIF?		☐ Yes	☐ No	☐ N/ A
	If yes, SCIF ID:	If no, explain how SCI is protected when the aircraft is unoccupied:			

2.	**Access Control:** How is access to the aircraft controlled?			
	a. By Guard Force	☐ Yes ☐ No	If yes, what is their security clearance level?	
	b. Is Guard Force Armed?		☐ Yes	☐ No
	c. By Assigned Personnel:		☐ Yes	☐ No
	If Yes, do personnel have visual control of the entrance door?	☐ Yes	☐ No	☐ N/ A
	d. When processing SCI, are all personnel aboard the aircraft cleared for all the SCI compartments that the aircraft is accredited for?		☐ Yes	☐ No
	If not, what are the procedures for segregating/ protecting SCI compartments from unauthorized disclosure?			

3.	**Hatches and Doors Leading Inside the Aircraft:**			
	a. Are doors equipped with GSA approved locks?		☐ Yes	☐ No
	Manufacturer	**Model**	**Group**	
	b. Are tamper serialized seals used when aircraft is unoccupied?		☐ Yes	☐ No
	If yes, are seals installed and a log book maintained by SCI cleared personnel?		☐ Yes	☐ No
	c. Remarks			

4.	**Acoustical Isolation**			
	a. Is a physical perimeter established around the aircraft at a distance so as to prevent inadvertent disclosure of SCI discussions or briefings from within the aircraft		☐ Yes	☐ No
	b. In instances where the physical perimeter barrier is not sufficient to control voices or sounds, are sound countermeasure devices or sound generating devices used?		☐ Yes	☐ No
	c. Remarks			

5.	**Visual Isolation**		
	a. Are doors or other openings in the aircraft through which the interior may be viewed screened or curtained?	☐ Yes	☐ Yes
	b. Remarks		
6.	**Procedures For Protecting SCI When The Aircraft Is Parked In Friendly/Unfriendly Territories**		

Section C: Intrusion Detection Systems (IDS)			
1.	**Is the aircraft equipped or located within a structure or area that has an IDS?**	☐ Yes	☐ No
	If yes, please provide the following:		
	a. IDS Company provider name *(if applicable)*		
	b. Premise Control Unit (PCU)		

Manufacturer	Model Number	Tamper Protection	☐ Yes	☐ No

c. Where is the PCU located?			
d. Location of interior motion detection protection: Accessible points of entry/ perimeter?	☐ Yes	☐ No
e. Has the IDS Alarm Monitor Station been installed to Underwriters Laboratories certified standards?	☐ Yes	☐ No
If yes, please provide certification number and expiration date of UL certification		

Certification Number	Expiration Date

f. Has the IDS passed CSA or UL 2050 installation and acceptance tests?	☐ Yes	☐ No
If yes, please attach a copy of certificate and skip to question 2 below. (Non -commercial proprietary system must answer all questions)		
g. Motion Sensors (Indicate sensor placement on a legible floor plan; 8.5'' x 11'' or 11'' x 17'' paper		

Manufacturer	Model Number	Tamper Protection	☐ Yes	☐ No

h. Are motion sensors installed above the false ceiling?	☐ Yes	☐ No	☐ N/ A

i. Are motion sensors installed below the false floors?	☐ Yes	☐ No	☐ N/ A

j. Are there any other intrusion detection equipment sensors/ detectors in use?	☐ Yes	☐ No

If yes, please identify make, model, and manufacturer and function (indicate on floor plan)

Make	Model	Manufacturer	Function

k. Does the IDS extend beyond the SCIF perimeter?	☐ Yes	☐ No
Can the status of PCU be changed from outside IDS protection?	☐ Yes	☐ No
If yes, is an audit conducted daily?	☐ Yes	☐ No
Has the IDS configuration been approved by the CSA?	☐ Yes	☐ No
l. Do any intrusion detection equipment components have audio or video capabilities?	☐ Yes	☐ No

If yes, please explain:		
Has the CSA mitigated this capability?	☐ Yes	☐ No
m. IDS Administrator SCI indoctrinated?	☐ Yes	☐ No
n. External Transmission Line Security: What is the method of line security? Meets NIST; FIPS AES Encryption?	☐ Yes	☐ No
If yes, has the encryption been certified by National Institute of Standards and Technology (NIST) or another independent testing laboratory?	☐ Yes	☐ No
If not NIST FIPS AES, is there an alternate?	☐ Yes	☐ No
If yes, please explain:		
Does the alternate line utilize any cellular or other Radio Frequency (RF) capability?	☐ Yes	☐ No
If yes, provide manufacturer and model		

Manufacturer	Model

o. Does any part of the IDS use a local or Wide Area Network?	☐ Yes	☐ No	☐ N/ A
(1) Is the Network Intrusion Detection Software (NIDS) administrator at least Top Secret (collateral) cleared?	☐ Yes	☐ No	☐ N/ A
(2) Is the host computer dedicated solely for security purposes?	☐ Yes	☐ No	☐ N/ A
(3) Is the host computer secured within an alarmed area controlled at the Secret or higher level?	☐ Yes	☐ No	☐ N/ A

(4) Is the host computer protected through firewalls or similar devices?	☐ Yes	☐ No	☐ N/A	
Are the firewalls/ devices configured to only allow data transfers between IDS components?	☐ Yes	☐ No	☐ N/A	
(5) Is the password for the host computer unique for each user and at least 8 characters long?	☐ Yes	☐ No	☐ N/A	
(6) Is the password changed semi-annually?		☐ Yes	☐ No	
(7) Are remote security terminals protected the same of the host computer?	☐ Yes	☐ No	☐ N/A	
If no, please explain:				
p. Was the IDS installed by U.S. citizens:	☐ Yes	☐ No	☐ N/A	
If no, please explain:				
q. Is emergency power available for the IDS?	☐ Yes	☐ No	☐ N/A	
What type? Generator	☐ Yes	☐ No	If yes, how many hours? _____	
What type? Battery	☐ Yes	☐ No	If yes, how many hours? _____	
r. If applicable, describe the method of ventilation and duct work protection:				

s. Where is the IDS Alarm Monitor Station located?			
t. Does the Monitor Station have any remote capabilities (i.e., resetting alarms, issuing PINs, accessing/ securing alarms, etc.)?	☐ Yes	☐ No	☐ N/A
If yes, please explain:			
u. Does the IDS have any automatic features (i.e., timed auto-secure, auto-access capabilities)?	☐ Yes	☐ No	☐ N/A
v. Does the PCU/ keypad have dial out capabilities?		☐ Yes	☐ No
w. IDS Response Personnel			
(1) Who provides initial alarm response?			
(2) Does the response force have a security clearance?		☐ Yes	☐ No
If yes, what is the clearance level:			
(3) Do you have a written agreement for external response force?		☐ Yes	☐ No
(4) Emergency procedures documented?		☐ Yes	☐ No
(5) Reserve security force available?		☐ Yes	☐ No

	(6) Response to an alarm condition	_____minutes	
	x. Are response procedures tested and records maintained?	□ Yes	□ No
	If no, please explain:		
	y. If required, has a Catastrophic Failure Plan been approved by the CSA?	□ Yes	□ No
	z. Does the IDS undergo semiannual testing?	□ Yes	□ No
	aa. Have IDS records been maintained:	□ Yes	□ No
	bb. Remarks		

	Section D: Classified Destruction Methods		
1.	For home station, describe the method and equipment used for destruction of classified/ sensitive material (if more than one method or device, use Remarks section to describe (if more than one, use Remarks section to list all manufacturer and model)		

Method	Device Manufacturer	Model

2.	Is a secondary method of destruction available	□ Yes	□ No
3.	Describe the location of destruction site(s) in relation to the aircraft?		
4.	Describe the method or procedure used for handling non -soluble classified/ sensitive material at your facility?		
5.	Do you have a written Emergency Action Plan (EAP) approved by CSA?	□ Yes	□ No
6.	Describe procedures for in-flight emergency destruction:		
7.	Remarks		

	Section E: TEMPEST/Technical Security			
1.	Does the aircraft electronically process classified information?		□ Yes	□ No
	If yes, what is the highest level of information processed?			
2.	Has it received TEMPEST accreditation?	□ Yes	□ No	□ N/ A
	Date	Accreditation granted by:		