

ATTACHMENT D

FLIGHT DYNAMICS SUPPORT SERVICES II

**DD FORM 254, CONTRACT SECURITY
CLASSIFICATION SPECIFICATION
TO BE PROPOSED (TBP)**

**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 SAFEGUARDING 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 TBD		a. ORIGINAL (Complete date in all cases)		Date (Y/M/D)
b. SUBCONTRACT NUMBER		b. REVISED (Supersedes all previous specs)	Revision No.	Date (Y/M/D)
c. SOLICITATION OR OTHER NUMBER NNG13449004R	DUE DATE (Y/M/D)	c. FINAL (Complete Item 3 in all cases)		Date (Y/M/D)

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 contractors request dated _____, retention of the identified classified material is authorized for a period of: _____

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)

a. NAME, ADDRESS, AND ZIP	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
---------------------------	--------------	--

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
---------------------------	--------------	--

8. ACTUAL PERFORMANCE

a. LOCATION NASA/Goddard Space Flight Center Greenbelt, MD 20771 and other NASA facilities and installations	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
--	--------------	--

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT
Flight Dynamics Support Services II (FDSS II)

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		<input checked="" type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTORS FACILITY OR GOVERNMENT ACTIVITY	<input checked="" type="checkbox"/>	
b. RESTRICTED DATA		<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input checked="" type="checkbox"/>	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FORMERLY RESTRICTED DATA		<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		<input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY	<input checked="" type="checkbox"/>	
(1) Sensitive Compartmented Information (SCI)	<input checked="" type="checkbox"/>		f. HAVE ACCESS TO US CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		<input checked="" type="checkbox"/>
(2) Non-SCI	<input checked="" type="checkbox"/>		g. BE AUTHORIZED TO USE THE SERVICES OF THE DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		<input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION		<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT		<input checked="" type="checkbox"/>
g. NATO INFORMATION		<input checked="" type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS		<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION		<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		<input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION		<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		<input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>		l. OTHER (Specify)	<input checked="" type="checkbox"/>	
k. OTHER (Specify)					
Sensitive But Unclassified (SBU)	<input checked="" type="checkbox"/>				

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)

NASA Goddard Space Flight Center, Public Affairs Office, Code 130, Greenbelt, MD 20771

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 the 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.)

In performance of this contract, some personnel may require access to classified information up to and including TOP SECRET. The contractor must have a sufficient number of cleared employees assigned duties under this contract to be able to complete all classified work assignments up to and including TOP SECRET.

- a. Space Network Security Classification Guide dated January 1, 2010
- b. National Industrial Security Program Operating Manual (NISPO), DOD 5220.22-M, dated February 28, 2006
- c. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7000, Tempest Countermeasures for November 1993
- d. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4000, Series on Communications Security September 1996
- e. COMSEC Supplement to former Industrial Security Manual, DOD 5220.22-S, current edition.
- f. OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources
- g. NPD 2810.1D, NASA Information Security Policy
- h. NPD 2810.1A, Security of Information Technology
- i. Federal Information Security Management Act of 2002
- j. Security Handbooks, Manuals, Regulations, Instructions, Directives, and Guidelines (current editions) for NASA Headquarters, GSFC as other applicable policies and procedures as identified by NASA.

SEE PAGE #3

14. ADDITIONAL SECURITY. Requirements, in addition to NISPOM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies additional requirements. Provide a copy of the requirements to the See Page #3) NO YES

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If yes, explain and identify specific areas or YES NO

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 Jeffrey W. Barrett	b. TITLE Industrial/Information Security Specialist	c. TELEPHONE (Include Area Code) 301.286.0725
--	--	--

d. ADDRESS (Include Zip Code)
NASA/GODDARD SPACE FLIGHT CENTER CODE
240 GREENBELT, MD 20771

e. SIGNATURE
Jeffrey W. Barrett

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

Item #14. Additional Security Requirements and/or Guidance

- k. Internet Protocol Operational Network (IONet) Security Policy, 700-DOC-029
- l. Internet Protocol Operation Network (IONet) Access Control Compliance Checklist, Revision 3
- m. NPR 1600.1, NASA Security Program Procedural Requirements w/Change 2
- n. NPR 1620.2, Physical Security Vulnerability Risk Assessments
- o. NPR 1620.3, Physical Security Requirements for NASA Facilities and Property
- p. NPD 1660.1B, NASA Counterintelligence (CI) Policy
- q. NPR 1660.1, NASA Counterintelligence (CI/Counterterrorism (CT) Program Procedural Requirements
- r. Homeland Security Presidential Directive /HSPD-5, National Incident Management System
- s. Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection
- t. Homeland Security Presidential Directive/HSPD-8, National Preparedness
- u. Homeland Security Telecommunications Systems Security HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors
- v. National Security Telecommunications Systems Security Instruction 4005
- w. NASA Central Office of Record Standard Operating Procedure (CSOP)

NASA officials will provide additional security, technical, and/or classification guidance. Requests concerning clarification or interpretation regarding security requirements under this contract will be directed to the NASA/GSFC Industrial Security Specialist. The place of performance will be at the contractor cleared facilities, GSFC and other locations where the requirement is covered by the obligations specified in Section C of the basic document.

Any employee, who observes or becomes aware of the deliberate or suspected compromise of classified national security information shall promptly report such information personally to the GSFC Counter Intelligence (CI) Office. If unclassified but sensitive information appears compromised by or on behalf of foreign or domestic powers, organizations or persons, employees shall report such information to the GSFC CI Office. If an employee becomes aware of information pertaining to international or domestic terrorist activities, employees shall also report to the GSFC CI Office. If the information indicates a computer compromise or other cyber intrusion, the Office of Inspector General shall be promptly notified.

Sensitive Compartmented Information

This contract requires access to Sensitive Compartmented Information (SCI). SCI will only be released to contractor employees requiring access in order to perform within the scope of the contract and only after official verification of the appropriate clearance level has been obtained. Any SCI material furnished to the contractor will be returned to the direct custody of the agency having cognizance unless other disposition instructions have been issued.

The names of any additional employees requiring SCI clearance solely for the purpose of this contract will be provided to a designated contract monitor or the Contracting Officer's Technical Representative (COTR), who will verify and approve the request. After approval, the name will be provided to the GSFC Security Division (GSD) Program Security Official for coordination with the Contractor Special Security Officer (CSSO). The CSSO shall submit a request for the investigation and clearance in accordance with the National Industrial Security Program Operating Manual and any additional instructions of the User Agency having cognizance.

Need-to-know verification for employees' classified visits to SCI facilities in the performance of this contract shall be obtained by the CSSO from the designated contract monitor, the COTR, or the GSD Program Security Official prior to submission or transmittal.