RFP: JTH24003

NSPA SECURITY ASPECTS LETTER

1. In the performance of this contract, the prime Contractor and any Sub-contractor(s) are required to comply with NATO security regulations as implemented by the National Security Authority (NSA) of the nation in which the work is performed.

2. All classified information and material shall be protected in accordance with the requirements established by the NSA of the nation in which the work is performed.

3. In particular, the contractor shall:

   a. develop and implement the security measures in relation to the Request For Proposals (RFP), contract or sub-contract;

   b. within 30 calendar days of Contract Award (CA), submit to the NSPA Security Officer the personal particulars of the persons the contractor wishes to employ on the project with a view to obtaining Personnel Security Clearances (PSCs) at the required level. No clearance or waiver to this requirement shall be granted; no Contractor personnel shall be assigned without having the needed clearance in place;

   c. maintain, a continuing relationship with the NSA and / or the Contracting Authority in order to ensure that all NATO classified information involved in the bid, contract or sub-contract is properly safeguarded;

   d. abstain from copying of any classified materiel (including documents) by any means, without first obtaining NSPA's permission, any classified materiel (including documents) entrusted to him by NSPA;

   e. supply the NSA, when so requested by the latter, with any information on the persons who will be required to have access to NATO classified information concerning the contract;

   f. maintain a record of his employees taking part in the project and who have been cleared for access to NATO classified information. This record must show the period of validity and the level of the clearances;

   g. deny access to NATO classified information to any persons other than those authorized to have access by the NSA;

   h. limit the dissemination of NATO classified information to the smallest number of persons as is consistent with the proper execution of the contract or sub-contract;

   i. comply with any request that persons to be entrusted with NATO classified information sign a statement undertaking to safeguard that information and signifying their understanding of their obligations under national legislation on the safeguarding of classified information, and that they recognize that they may have comparable obligations under the laws of the other NATO nations in which they may have access to classified information;

j. report to the NSPA Security Officer and to his NSA any breaches or suspected breaches of security, suspected sabotage or subversive activity, any breach giving rise to doubts as to the trustworthiness of an employee, any changes in the ownership, supervisory or managerial staff of the facility or any changes that affect the security arrangements and security status of the facility, and any other information which may be required by the NSA, such as reports on holdings of NATO classified information or materiel;

k. obtain the approval of NSPA before beginning negotiations with a view to sub-contracting any part of the work which would involve the Sub-contractor having possible access to NATO classified information, and to place the Sub-contractor under appropriate security obligations which in no case may be less stringent than those provided for his own contract;

l. undertake not to utilise, other than for the specific purpose of the bid, contract or sub-contract, without the written permission of NSPA, any NATO classified information supplied to him, and return to NSPA all classified information referred to above, as well as that developed in connection with the contract or sub-contract unless such information has been destroyed, or its retention has been duly authorized by the contracting office or the sub-contracting officer. Such NATO classified information shall be returned at such time as the contracting office may direct; and

m. comply with any procedure established with respect to the dissemination of NATO classified information in connection with the contract or sub-contract.

4. Any person taking part in the performance of work the classified parts of which are to be safeguarded, must possess the appropriate NATO security clearance issued by his NSA. The level of this clearance must be at least equal to the security category of the materiel, the related information or specifications.

5. Unless specifically authorized to do so by NSPA, the Contractor may not pass on any NATO classified information to any third party to whom a request to supply goods or services has been submitted.

6. No change in level of classification or de-classification of documentation or materiel may be carried out unless written authority in this respect is obtained from NSPA .

7. No CIS may be used for processing classified information without prior accreditation by the responsible authorities.

8. Failure to implement these provisions and the security regulations established by the NSA of the nation where the contractual work is being performed may result in termination of this contract without reimbursement to the Contractor or claim against NATO, NSPAor the national government of the said nation.

9. The attached NSPA Security Requirements Check List (SRCL) document indicates the degree of classification of the data and materiel (equipment, information, technical manuals, specifications) which may be handled in the performance of work under this contract and which must be safeguarded in accordance with the provisions of this letter.

10. The transportation/return of NATO classified material from private firms to NSPA is to be performed on the firms' initiative through their national security authorities.

11. The Contractor shall be required to acknowledge receipt of an accompanying SAL that is made part of the applicable contract and confirm that it understands the security aspects defined.

Security Requirements Checklist (SRCL)

ITEMS APPLICABLE: ALL SERVICES INCLUDED IN RFP JTH24003

	SUBJECT	Security Classification Level	Remark N°
1	CONTRACT /RFP N°:	NU	
2	GENERAL DESCRIPTION OF ITEMS IN THIS CONTRACT	NU	1
2A	DETAILED DESCRIPTION OF INDIVIDUAL ITEMS	NU	1
3	EXISTENCE OF CONTRACT	NU	1
4	COMPLETE EQUIPMENT	Up to NS	2
5	DRAWINGS AND SKETCHES	Up to NR	1
6	SPECIFICATIONS	Up to NR	1
7	DESIGN CALCULATION	Up to NR	1
8	TEST AND PERFORMANCE DATA	Up to NS	1
9	ASSEMBLIES AND SUB-ASSEMBLIES	Up to NR	1
10	TEST EQUIPMENT	Up to NR	1
11	SUB-CONTRACTS	Up to NS	2, 3
12	TECHNICAL REPORTS	Up to NR	1
13	PROGRESS REPORTS AND PRODUCTION REPORTS	NU	1
14	INSTALLATIONS	Up to NR	1
15	OPERATING INSTRUCTIONS	Up to NS	1
16	MAINTENANCE INSTRUCTIONS	Up to NC	1
17	PARTS LIST	Up to NR	1
18	PACKAGING AND PACKING INSTRUCTIONS	NU	
19	SHIPPING INSTRUCTIONS	NU	
20	QUANTITIES	NU	
21	ACCESS TO SITES	Up to NS	4

Remark No 1: The Ship's Combat System, and integrated sub-systems, shall operate and handle information up to NS security classification level. Any design, photo, or report which does not reveal or provide details to the degree that classified information can be derived shall be unclassified.
Remark No 2: The subsystems of the Ship's Combat System would need to handle different level of information, i.a.w. provisions of SOW, up to and including NS (see also Remark No 1).
Remark No 3: The level of classification of data handled in the framework of subcontracts will depend on the goods and services requested in the framework of those specific sub-contracts, and will be within the limits established per each line in this table.
Remark No 4: The level of classification required for access to site will depend on the site content, and will be within the limits established per each line in this table (see also Remark No 1).

Form: 786