

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 SAFEGUARDING REQUIRED TOP SECRET
--	---

2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
a. PRIME CONTRACT NUMBER		X	a. ORIGINAL (Complete date in all cases) DATE (YYMMDD) 02 04 22
b. SUBCONTRACT NUMBER		b. REVISED (Supersedes all previous specs)	Revision No. DATE (YYMMDD)
c. SOLICITATION OR OTHER NUMBER	DUE DATE (YYMMDD)	c. FINAL (Complete item 5 in all cases)	DATE (YYMMDD)

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 identified classified material is authorized for the period of _____

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

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

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	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT
Next Generation Engineering Contract (NexGen) - provides support for the engineering and interoperability of DISA's core mission areas.

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 CONTRACTOR'S FACILITY OR A 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	<input checked="" type="checkbox"/>	
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 U.S. 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 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)		
k. OTHER (Specify) SIOP-ESI	<input checked="" type="checkbox"/>		All persons gaining access must be U.S. Citizens. Personnel authorized access to and courier of cryptographic equipment.	<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*):

DISA DITCO-NCR and Public Affairs. Also see DFARS Clause 252.204-7000, Disclosure of Information. Public release of SCI/SAP material is not authorized.

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.*)

Pre-award access is not required. This DD Form 254 reflects the security requirements for the contract when awarded.

See Attached Continuation Sheet

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM 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 the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.*) YES NO

The Contractor will abide by DIAMs 50-4 and 50-5, Volumes I and II and DCID 1/21.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (*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.*) YES NO

DISA SSO (ISBE) will e responsible for inspection of SCI 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 RHONDA KIRBY LaGARDE	b. TITLE Contracting Officer	c. TELEPHONE (<i>Include Area Code</i>) (703) 681-1250
--	---------------------------------	---

d. ADDRESS (*Include Zip Code*)
 Defense Information Systems Agency
 5211 Leesburg Pike, Skyline 5, Suite 900A
 Falls Church, VA 22041

e. SIGNATURE

17. REQUIRED DISTRIBUTION	
<input checked="" type="checkbox"/>	a. CONTRACTOR
<input type="checkbox"/>	b. SUBCONTRACTOR
<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
<input type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY

Reference Item 10a: Contractor is authorized to receive Government furnished cryptographic equipment. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. Further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior approval of the contracting activity.

Classified paper COMSEC material may be destroyed by burning, pulping or pulverizing. When a method other than burning is used, all residue must be reduced to pieces 5-mm or smaller in any dimension. When classified COMSEC material other than paper is to be destroyed, specific guidance must be obtained from the COMSEC custodian.

Contractor will not incorporate COMSEC in any documentation.

Reference Item 10c: This contractor is permitted access to CNWDI in performance of the contract. The Government program manager or designated representative ensures the contractor security supervisor is briefed for access to CNWDI by a Government representative prior to granting access.

Reference Item 10e(1): This contract requires access to SCI:

a. The Director, Defense Intelligence Agency (DIA) and Director, Defense Information Systems Agency (DISA), as the executive agents for DIA, have exclusive security responsibility for SCI released to the contractor or developed under this contract.

b. Contractor generated or Government furnished material may not be provided to the Defense Technical Information Center (DTIC). Contract generated technical reports will bear the statement "Not Releasable for the Defense Technical Information Center per DoD Instruction 5230.24".

c. All contractor personnel requiring access to SCI information must: be U.S. citizens, have been granted a final Top Secret security clearance by the U.S. Government, have been approved as meeting DCID 1/14 criteria by a Government Cognizant Security Agency, and have been indoctrinated for the applicable compartments of SCI access prior to being given any access to such information released or generated under this contract. Immigrant aliens, interim cleared personnel, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract without the expressed permission of the Director, DISA (through the DISA CISS Security and Certification Department SSO) and the Director, DIA.

d. Classified Material released or generated under this contract is not releasable to foreign nations without the expressed written permission of the Director, DISA (SSO) and Director, DIA.

e. Recipients of SCI under this contract may not be released to subcontractors without permission of the DISA SSO.

f. Unclassified information under this contract may not be released to subcontractors without permission of the Contracting Officer and coordination with the DISA CISS Security Programs and Oversight Division (ISBE).

g. STU-III terminals installed at the contractor's facilities shall be supported by a COMSEC account (of the contractor of DISA). STU-IIIs in SCI Facilities (SCIFs) require Class VI Cryptographic Ignition Key (CIK).

Reference Item 10f: To execute this contract, additional security requirements in addition to DoD 5220.22-M will be required. The contractor shall comply with the security provisions of these programs. Marking and/or classification guidance for material originated or generated under this contract will be provided through the DISA CISS Security Operations Division (ISBE) under separate cover. Any material generated by the contractor (including correspondence, drawings, models, mockups, photographs, schematics, progress, special and inspection reports, engineering notes, computations and training aids) shall be classified according to content. Guidance for classification shall be derived from the applicable Security classification Guides, Government furnished equipment or data, or special instructions. Such material shall not contain contractor logos or similar identifiers, which identify specific contractor or team members.

Reference Item 10f and 11c: This contract will be performed in a facility approved through the DISA CISS Security Programs and Oversight Division (ISBE) in accordance with applicable SAP security requirements. The CSO (DIS) may be relieved of security cognizance for the SAO by the DISA CISS/ISBE Security Programs and Oversight Division and/or the SAP Program Management Office (PMO) which will have responsibility for all SAP material or information released to the contractor under this contract.

Reference Item 10e(1) and 10f: Upon expiration of this contract, the contractor shall request disposition instructions for all classified and unclassified project material. The contractor may be directed to properly destroy the material or return it. If classified or unclassified project material is to be retained by the contractor, every effort should be taken to transfer it to a follow-on contract or similar effort, if applicable. This must be done however, with the Contracting Officer approval. Unless written authorization by the Contracting Officer to retain specific material for a specific period of time is received, the material shall be returned or destroyed as instructed. Any exception to security policy shall be referred to the CSO/DISA CISS Security programs and Oversight Division (ISBE) for coordination with the appropriate agencies and the Contracting Officer.

Reference Item 10g: Access up to and including NATO SECRET material will be required for reference only at the Government facility.

Reference Item 10i: The contract requires access to Limited Dissemination Information (LIMDIS); restrictive controls established by an Original Classification Authority (OCA) to emphasize need-to-know protective measures available within the regular security system. LIMDIS will not be reproduced. Disclosure of information will require prior permission of originator.

Reference Item 10j: "For Official Use Only" (FOUO) information provided to the contractor under this contract shall be safeguarded as specified in DoD 5400.7, DoD Freedom of Information Act Program, Chapter 4.

Reference Item 10k: This contract requires that specified contractor employees be granted access to Single Integrated Operational Plan – Extremely Sensitive Information (SIOP-ESI). Employees requiring SIOP-ESI access will be processed as follows:

- a. The DISA COR will forward to the DISA Security Programs and Oversight Division (ISBE), via an Interoffice Memorandum (IOM) a request to process certain employees of the company for SIOP-ESI access. The request will be marked with the appropriate markings (i.e., justification). This request will contain the following:
 1. Name and SSN of the employee(s).
 2. Company name, address, CAGE code, telephone number.
 3. Date and place of birth for employee(s).
 4. Citizenship of employee(s).
 5. Citizenship of employee's spouse.
 6. SIOP-ESI Category required.
 7. Employee's clearance level and date, investigation type and date.
 8. Inclusive dates SIOP access will be required.
 9. Contract number.
 10. Contract expiration date.
 11. Contract review date.
 12. Justification for requesting SIOP-ESI access.
- b. DISA CISS Security Programs and Oversight Division (ISBE) will forward a letter to certify the need-to-know for SIOP-ESI access to the FSO at the company via DISA Form Letter 16.
- c. When temporary access to SIOP-ESI has been approved by the Joint Chief's of Staff, the DISA CISS Security and Certification Department (ISBE) will forward this information to the FSO and authorize the employee to be briefed for access.
- d. The FSO is responsible for notifying the DISA CISS Security Programs and Oversight Division (ISBE) when the employee is transferred from one facility to another within the company, when the employee's employment is terminated, when they resign, or have been transferred and do not require continued access.
- e. The FSO is responsible for ensuring that the employee completes the required security forms for submission to the DIS Clearance Office (DISCO) in a timely manner.
- f. Information that an individual has been granted access to SIOP-ESI is unclassified.

Reference Item 11c: No contractor SCIF is required. Visit requests by contractors shall be forwarded to the applicable task monitor (TM) for approval and Need-to-Know certification before being sent to the facility to be visited. The TM must be notified and approve the receipt or generation of all classified information under the applicable task order. All classified information received or generated under this contract is the property of the U.S. Government. At the expiration or termination of a task order, the U.S. Government will be contacted for proper disposition instructions.

Reference Item 11d: Detailed information will be provided in the individual task order statement of work.

Reference Item 11f: Access to classified information in the following locations outside the U.S., Puerto Rico, U.S. Possessions and Trusted Territories may be required in the performance of this contract: Germany, Belgium, Japan, Korea. Detailed information will be provided in the individual task order statement of work.

Reference Item 11g:

- a. The Contractor must prepare and forward DD Forms 1540 and 1541 to the COR for authorization BEFORE the services may be requested.
- b. Technical information on file at the Defense Technical Information Center (DTIC) will be made available to the contractor if the contractor requires such information. The contracting officer will certify the field of interest relating to the contract.

Reference Item 11i: The contractor shall not process classified information by electrical means prior to a DISA TEMPEST evaluation of the equipment/systems and facility, and written DISA certification that the facility meets DISA TEMPEST criteria. In order to expedite the DISA TEMPEST evaluation, the contractor shall provide a list of equipment, to include model number that is associated with the processing of classified information. In addition, the estimated percentage of classified information processed, cable/conduit runs, a floor plan layout that depicts placement of equipment in relation to other rooms, equipment distances from walls or uncontrolled areas, and physical security being afforded the equipment both during processing and after hours. The above TEMPEST evaluation and DISA approval will not be required if previous DISA approval can be furnished and is no more than 2 years old. The existing approval must be for processing information at the same or higher level and at the same facility and items of equipment.

The following guidance applies to contractor owned electronic equipment and systems used to process classified information relating to this contract:

- a. When electronic equipment is used to process classified information, a written TEMPEST Assessment/Risk Analysis must be provided to the CO, or his/her designated representative, for review and approval.
- b. If only CONFIDENTIAL information will be processed, additional TEMPEST countermeasures will not be required. However, the contractor must maintain records of the amount of CONFIDENTIAL information processed for periodic review of the Contracting Agency.
- c. If SECRET or TOP SECRET information will be processed, TEMPEST countermeasures will be applied only when a clear and compelling requirement exists. The completed TEMPEST Assessment/Risk Analysis will be used by the Contracting Agency to evaluate the need for additional TEMPEST countermeasures.

TEMPEST requirements for government furnished equipment or for electronic equipment developed, manufactured, or assembled for the Government by the contractor will be provided separately.

Reference Item 11k: Contractor employees or cleared commercial carriers shall not carry classified COMSEC material on commercial passenger aircraft anywhere in the world without approval of the Procuring CO. The COR requests services from the Commander, DCS, ATTN: Operations Division, Fort George G. Meade, MD 20755-5370. Only certain classified information qualifies for shipment by DCS. It is the responsibility of the contracting activity to comply with DCS policy and procedure.

Reference Item 15. DIS will forward a copy of all inspection results to DISA (Security Division, ISBE), 5113 Leesburg Pike, Falls Church, VA 22041-3230.