F33657-01-D-2071
Section J Attachment 2
18 JUN 01

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: Secret

b. LEVEL OF SAFEGUARDING REQUIRED: Secret

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

X	a. PRIME CONTRACT NUMBER: F33657-01-D-2071/Exp date 031231	
	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)* 20010618
	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 [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	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
ECC International Corp. 2001 W. Oak Ridge Road Orlando FL 32809-3803	54206	DSS Southeast Region 2300 Lake Park Dr STE 250 Smyrna GA 30080-7606

7. SUBCONTRACTOR

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

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
N/A	N/A	N/A

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Training Systems Acquisition (TSA) Indefinite Delivery/Indefinite Quantity (ID/IQ) Contract for the continued acquisition of USAF, DoD Customer, and Foreign Military Sales (FMS) Training Systems

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)*		X
k. OTHER *(Specify)*		X			

F33657-01-D-2071
Section J Attachment 2
18 JUN 01

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 [X] Through *(Specify)*

ASC/PA 1865 W Fourth St Room 240 - WPAFB OH 45433-7129

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 classifiection 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.)*

The National Industrial Security Program Operating Manual (NISPOM), January 1995 applies to this contract.

This is an ID/IQ contract and each delivery order requires a separate and specific DD Form 254 for the work to be performed.

a. Ref Blk 10e(2): Contractor will require access to intelligence information and must comply with AFI 14-303/AFMC Supplement 1. The Program Manager has determined that disclosure does not create an unfair competitive advantage for the contractor or a conflict of interest with the contractor's obligation to protect the information and will submit the AFMC Form 210 to the local SIO for approval prior to granting access.
b. Ref Blk 10j: For Official Use Only applies. See Addendum.
c. Ref Blk 11c: Any classified information generated in the performance of this contract shall require the contractor to apply derivative classification and markings consistent with the source material. Special considerations apply. See addendum.
d. The transfer of documents to other contracts or IR&D efforts is not permitted without the written consent of the ASC/YW Contracting officer.
e. Program Manager: Each individual delivery order will identify the program manager.
f. ACO Manager: As identified in the specific DD Form 254.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. [X] 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 requirements to the cognizant security office. Use Item 13 if additional space is needed.)
This contract requires the contractor to comply with the provisions of the Training Systems Product Group Program Protection Plan, 15 May 1999.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. [ ] Yes [X] 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.)

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)*
Sandra Geib	Contracting Officer	(937) 255-7388 ext. 249

d. ADDRESS *(Include Zip Code)*
ASC/YWI
2240 B Street, Building 11, Room 150
WPAFB OH 45433-7111

e. SIGNATURE
Sandra Geib

88SFS/SFAS
COORDINATION
PC-ONLY
Ellen [illegible]

17. REQUIRED DISTRIBUTION

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

88th SFS/SFAS Bldg 8)
1801 TENTH ST ROOM 103
WPAFB OH 45433-7625

DD FORM 254 (BACK), DEC 1999

F33657-01-D-2071
Section J Attachment 2
18 JUN 01

ADDENDUM TO DD FORM 254 (Block 10j)
FOR OFFICIAL USE ONLY (FOUO)

(Reference DoD Regulation 5400.7/Air Force Supplement, 22 July 1999.)

1. **GENERAL:** FOUO is information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from the public because disclosure would cause a foreseeable harm to an interest protected by one or more of the Freedom of Information Act (FOIA) exemptions 2 through 9. Additional information on FOUO may be obtained by contacting the User Agency. FOUO is assigned to information at the time it is created in a DoD Agency or derivatively as instructed in a Security Classification Guide.

2. **MARKING:**

a. FOUO information received **(released by a DoD component)** should contain the following marking, when received: ***THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER FOIA. EXEMPTION(S) ___ APPLIES/APPLY.***

b. Mark an unclassified document containing FOUO information "FOR OFFICIAL USE ONLY" at the bottom of each page containing FOUO information and on the bottom of the front page or front cover (if any) and on the back of the last page and on the back cover (if any). Each paragraph containing FOUO information shall be marked as such.

c. Within a classified document, an individual page that contains both FOUO and classified information shall be marked at the top and bottom with the highest security classification of information appearing on the page. Individual paragraphs shall be marked at the appropriate classification level, as well as unclassified or FOUO, as appropriate. An individual page that contains FOUO information but no classified information shall be marked "FOR OFFICIAL USE ONLY" at the top and bottom of the page, as well as each paragraph that contains FOUO information. NOTE: For "production efficiency" the entire document may be marked top and bottom with the highest level of classification contained within it, as long as every paragraph is marked to reflect the specific classification of the information it contains.

d. Mark other records, such as computer print outs, photographs, films, tapes, or slides "FOR OFFICIAL USE ONLY" so that the receiver or viewer knows the record contains FOUO information.

e. Mark each part of a message that contains FOUO information. Unclassified messages containing FOUO information must show the abbreviation "FOUO" before the text begins.

3. **DISSEMINATION:** FOUO may be disseminated between officials of DoD Components, DoD contractors, consultants and grantees to conduct official business for DoD. Recipients shall be made aware of the status of such information **and transmission shall be by means that preclude unauthorized public disclosure.**

4. **TRANSMISSION:** FOUO information shall be transmitted in a manner that prevents disclosure of the contents. When not commingled with classified information, it may be sent via first-class mail or parcel post. Bulky shipments, i.e. testing materials, that otherwise qualify under postal regulations, may be sent by fourth-class mail. FOUO information may also be sent over facsimile equipment; however, when deciding whether to use this means, balance the sensitivity of the records against the risk of disclosure. Consider the location of sending and receiving machines and ensure authorized personnel are available to receive the FOUO information as soon as it is transmitted. Transmittal documents shall call attention to the presence of FOUO attachments. FOUO information may also be sent via e-mail, if it is sent via a system that will prevent unintentional or unauthorized disclosure.

5. **STORAGE:** To safeguard FOR OFFICIAL USE ONLY records during normal duty hours, place them in an out-of-sight location if your work area is accessible to persons who do not have a valid need for the information. After normal duty hours, store FOUO records to prevent unauthorized access. File them with other unclassified records in unlocked files or desks when normal internal building security is provided. When there is no internal building security, locked buildings or rooms normally provide adequate after-hours protection. If such protection is not considered adequate, FOUO material shall be stored in locked containers such as file cabinets, desks, or bookcases. *Expenditure of funds for security containers or closed areas solely for the protection of FOUO data is prohibited.*

6. **DESTRUCTION:** When no longer needed, FOUO information shall be disposed of by any method that will preclude its disclosure to unauthorized individuals.

F33657-01-D-2071
Section J Attachment 2
18 JUN 01

ADDENDUM TO DD FORM 254 (Block 11c)
SPECIAL CONSIDERATIONS
(AFSSM 7011 EXTRACT)

3.5. Special Items. People may innocently introduce other radio devices, such as pagers, hand-held portable transceiver radios, cellular telephones, cordless telephones, and cordless microphones into the area processing classified national security information with disastrous results. Also, alarm systems may use radio transmitters to alert remotely located security or fire-fighting teams.

3.5.1. Hand-Held Radios. Hand-held radio transceivers used with intrabase radios (sometimes abbreviated IBR) and land mobile radios (sometimes abbreviated LMR) deserve special consideration because of their unique operational applications. A person may carry these devices into an area where classified national security information is processed. If the person carrying such a device works in the facility, either turn off the device and use the telephone or separate it 2 meters from classified processors: no transmissions are allowed. If the person carrying the device is a short-term visitor, it is not necessary to turn off the radio because the visitor usually moves about in the facility. Infrequent transmissions are allowed, but only for short durations.

3.52. Beepers and Pagers. Beepers and pagers deserve special consideration because of their unique operational applications. A person may carry these devices into an area where classified national security information is processed. If the person carrying such a device works in the facility, either turn off the device and use the telephone or keep the device 2 meters from classified processors. If the person carrying the device is a short-term visitor, it is not necessary to turn off the device because the visitor usually moves about in the facility. If the device has a transmit capability, follow the instructions for hand-held radios.

3.5.3. Alarm Systems. The mode of operation of alarm systems radio frequency transmitters will determine their treatment. Any such transmitter with a continuous transmit mode or a high duty cycle (transmits most of the time) must meet the same separation requirements as all other fixed transmitters. If they do not meet these requirements, exclude them from operating in the classified national security information processing area. Low duty cycle (transmits short bursts infrequently) systems are not considered hazards and require no special treatment.

3.5.4. Cellular Telephones. When a cellular telephone is used as an operational necessity separate it 5 meters from RED equipment. When the cellular telephone is a personal asset, its use is prohibited. Disable the unit from receiving calls or separate it 10 meters from RED processors.

3.5.5. Cordless Telephones. When a radio frequency cordless telephone is used as an operational necessity, separate it 5 meters from RED equipment. When the cordless telephone is a personal asset, its use is prohibited. Disable the personal cordless telephone from receiving calls or separate it 10 meters from RED processors. There are no separation requirements for infrared cordless telephones.

3.5.6. Cordless Microphones.

3.5.6.1. Radio Frequency Cordless Microphones. When a radio frequency cordless microphone, encrypted or unencrypted, is used for briefing either classified national security information or unclassified information, separate it 10 meters from RED equipment. Using unencrypted radio frequency cordless microphones for classified briefings is prohibited.

3.5.6.2. Infrared Cordless Microphones. Using an infrared cordless microphone for briefing classified national security information requires a closed room: keep the doors closed and cover the windows with drapes.

3.5.7. Cordless Keyboards. When a radio frequency cordless keyboard is used, separate it 10 meters from RED equipment. Radio frequency cordless keyboards cannot be used to process classified national security information unless encrypted.

3.5.8 Wireless Local Area Networks. When a radio frequency wireless local area network is used, separate the transmitter and receiver units 10 meters from RED equipment.

The complete document can be obtained from the Air Force Information Protection Home Page (http://www.afca.scott.af.mil/gc/gci/).