DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the National Industrial Security Program (NISP) apply to all security aspects of this effort involving classified information.)

OMB No. 0704-0567
OMB approval expires: May 31, 2022

RETURN COMPLETED FORM AS DIRECTED IN THE INSTRUCTIONS.

1. CLEARANCE AND SAFEGUARDING

a. LEVEL OF FACILITY SECURITY CLEARANCE (FCL) REQUIRED *(See Instructions)*	b. LEVEL OF SAFEGUARDING FOR CLASSIFIED INFORMATION/ MATERIAL REQUIRED AT CONTRACTOR FACILITY
Secret	Secret

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

- ☐ **a. PRIME CONTRACT NUMBER** *(See instructions.)*
- ☐ **b. SUBCONTRACT NUMBER**
- ☒ **c. SOLICITATION OR OTHER NUMBER** 423630-BA-Basic-0-0-0 **DUE DATE** *(YYYYMMDD)* 20220427

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

- ☒ **a. ORIGINAL** *(Complete date in all cases.)* **DATE** *(YYYYMMDD)*
- ☐ **b. REVISED** *(Supersedes all previous specifications.)* **REVISION NO.** **DATE** *(YYYYMMDD)*
- ☐ **c. FINAL** *(Complete Item 5 in all cases.)* **DATE** *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? ☒ No ☐ Yes *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? ☒ No ☐ Yes *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(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*
N/A	N/A	N/A

7. SUBCONTRACTOR(S) *(Click button if you choose to add or list the subcontractors -- but will still require a separate DD Form 254 issued by a prime contractor to each subcontractor)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*
N/A	N/A	N/A

8. ACTUAL PERFORMANCE *(Click button to add more locations.)*

a. LOCATION(S) *(For actual performance, see instructions.)*	b. CAGE CODE *(If applicable, see Instructions.)*	c. COGNIZANT SECURITY OFFICE(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*
N/A	N/A	N/A

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT

This effort will provide the Air Force Technical Application Center (AFTAC) Meteorological Modeling and Analysis Mission (MMA) with updated software.

10. CONTRACTOR WILL REQUIRE ACCESS TO: *(X all that apply. Provide details in Blocks 13 or 14 as set forth in the instructions.)*

- ☐ **a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION**
- ☒ **b. RESTRICTED DATA**
- ☒ **c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)** *(If CNWDI applies, RESTRICTED DATA must also be marked.)*
- ☒ **d. FORMERLY RESTRICTED DATA**
- **e. NATIONAL INTELLIGENCE INFORMATION:**
  - ☒ **(1) Sensitive Compartmented Information (SCI)**
  - ☒ **(2) Non-SCI**
- ☐ **f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION**
- ☒ **g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION**
- ☐ **h. FOREIGN GOVERMENT INFORMATION**
- ☐ **i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION**
- ☒ **j. CONTROLLED UNCLASSIFIED INFORMATION (CUI)** *(See instructions.)*
- ☐ **k. OTHER** *(Specify)* *(See instructions.)*

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL: *(X all that apply. See instructions. Provide details in Blocks 13 or 14 as set forth in the instructions.)*

- ☐ **a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY** *(Applicable only if there is no access or storage required at contractor facility. See instructions.)*
- ☐ **b. RECEIVE AND STORE CLASSIFIED DOCUMENTS ONLY**
- ☒ **c. RECEIVE, STORE, AND GENERATE CLASSIFIED INFORMATION OR MATERIAL**
- ☐ **d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE**
- ☐ **e. PERFORM SERVICES ONLY**
- ☐ **f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S.,PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES**
- ☐ **g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER**
- ☒ **h. REQUIRE A COMSEC ACCOUNT**
- ☐ **i. HAVE A TEMPEST REQUIREMENT**
- ☐ **j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS**
- ☐ **k. BE AUTHORIZED TO USE DEFENSE COURIER SERVICE**
- ☒ **l. RECEIVE, STORE, OR GENERATE CONTROLLED UNCLASSIFIED INFORMATION (CUI).** *(DoD Components: refer to DoDI 5200.48, only for specific CUI protection requirements. Non-DoD Components: see instructions.)*
- ☐ **m. OTHER** *(Specify)* *(See instructions.)*

12. PUBLIC RELEASE

Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the National Industrial Security Program Operating Manual (NISPOM) or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for review and approval prior to release to the appropriate government approval authority identified here with at least office and phone contact information and if available, an e-mail address. *(See instructions)*

☐ **DIRECT** ☒ **THROUGH** *(Specify below)*

AFTAC/OPSEC, 1020 South Patrick Drive Patrick, SFB FL 32925-3516

Public Release Authority:

Contractor is to submit requests through the Contracting Officer for OPSEC Program manager review and public release authorization

13. SECURITY GUIDANCE

The security classification guidance for classified information needed for this 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. The field will expand as text is added. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. Also allows for up to 6 internal reviewers to digitally sign. See instructions for additional guidance or use of the fillable PDF.)

DD FORM 254 is invalid 31 Dec 2023

List of Attachments (All Files Must be attached Prior to Signing, i.e., for any digital signature on the form)

SSO Patrick	**NAME & TITLE OF REVIEWING OFFICIAL**	**SIGNATURE**
	Rebecca Lehnerz, Alt. Chief, Security Operations	LEHNERZ.REBECCA.1114593660 Digitally signed by LEHNERZ.REBECCA.L.1114593660 Date: 2022.04.30 12:51:02 -04'00'
ISPM	**NAME & TITLE OF REVIEWING OFFICIAL**	**SIGNATURE**
	Yvette Coleman Security Specialist	COLEMAN.GLORIA.YVETTE.1054872239 Digitally signed by COLEMAN.GLORIA.YVETTE.1054872239 Date: 2022.04.29 11:47:17 -04'00'
Information Assurance	**NAME & TITLE OF REVIEWING OFFICIAL**	**SIGNATURE**
	Natasha Miles, CISO	MILES.NATASHA.M.1075087493 Digitally signed by MILES.NATASHA.M.1075087493 Date: 2022.04.29 12:57:49 -04'00'

14. ADDITIONAL SECURITY REQUIREMENTS

Requirements, in addition to NISPOM requirements for classified information, are established for this contract.

☐ No ☒ Yes *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 CSO. The field will expand as text is added or you can also use item 13. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. (See instructions for additional guidance or use of the fillable PDF.)*

See attachment for Release of SCI Intelligence/Non-Intelligence Information (10.e.1.2) for additional security requirements. Prior approval of the contracting activity is required for subcontracting. All DD FMs 254 prepared for a subcontract by the prime contract will be forwarded to the government contracting monitor and SSO Patrick for signature prior to award of the subcontract. Access to intelligence information will require special briefings and final U.S. Government Top Secret clearance with ICD 704 eligibility.

15. INSPECTIONS

Elements of this contract are outside the inspection responsibility of the CSO.

☐ No ☒ Yes *If Yes, explain and identify specific areas and government activity responsible for inspections. The field will expand as text is added or you can also use item 13. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. (See instructions for additional guidance or use of the fillable PDF.)*

SSO Patrick has exclusive security responsibility for all SCI classified material released to or developed under this contract and held at the government SCI facility and/or the contractor's SCI facility. DCSA retains cognizance only over non-SCI material released to or developed under the contract and held within the contractor's cleared facility.

16. GOVERNMENT CONTRACTING ACTIVITY (GCA) AND POINT OF CONTACT (POC)

a. GCA NAME ARTURO TECSON	**c. ADDRESS** *(Include ZIP Code)* 1020 South Patrick Drive Patrick SFB, FL 32925	**d. POC NAME** Arturo Tecson
		e. POC TELEPHONE *(Include Area Code)* +1 (321) 494-8939
b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE *(See Instructions)* FA7022		**f. EMAIL ADDRESS** *(See Instructions)* arturo.tecson.1@us.af.mil

17. CERTIFICATION AND SIGNATURES

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. Upon digitally signing Item 17h, no changes can be made as the form will be locked.

a. TYPED NAME OF CERTIFYING OFFICIAL *(Last, First, Middle Initial)* *(See Instructions)* Batchelor, Laytesha	**d. AAC OF THE CONTRACTING OFFICE** *(See Instructions)* FA7022	**h. SIGNATURE**
b. TITLE Contracting Officer	**e. CAGE CODE OF THE PRIME CONTRACTOR** *(See Instructions.)*	
c. ADDRESS *(Include ZIP Code)* 1020 South Patrick Dive Patrick SFB, FL 32925	**f. TELEPHONE** *(Include Area Code)* +1 (321) 494-8950	**i. DATE SIGNED** *(See Instructions)*
	g. EMAIL ADDRESS *(See Instructions)* laytesha.batchelor.1@us.af.mil	

18. REQUIRED DISTRIBUTION BY THE CERTIFYING OFFICIAL

- ☒ **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. OTHER AS NECESSARY** *(If more room is needed, continue in Item 13 or on additional page if necessary.)*

ACCESS TO SENSITIVE COMPARTMENTED INFORMATION (SCI)

1. Inquiries pertaining to classification guidance on SCI will be directed to the responsible AFTAC Contracting Officer's Representative (COR), or Program Manager (PM) and the AFTAC Special Security Officer (SSO) as identified under Block 13 of the DD Form 254. (The term PM refers to PM and COR, in this document). SCI access is limited to the executable term of the contract which is identified in Block 13 of the DD 254. Upon expiration of the SCI contract, all contractors with SCI accesses must be withdrawn and all SCI materials must be recovered.

2. All SCI access required in the performance of this contract will be justified through the PM and maintained/approved by the SSO. The PM will provide the contractor Facility Security Officer (FSO) or contractor Special Security Officer (CSSO) with written approval of personnel and the necessary data to submit request(s) for single scope background investigations (SSBIs) IAW DOD 5220.22-M (NISPOM) and Supplement Overprint. Term certifications from any other government agencies for contractors working SCI portions of the AFTAC contracts are acceptable for the time between submission and approval of the contractor SCI access request. FSO/CSSO will be required to pass Personal Identifiable Information (PII) to the SSO; the contractor must make provisions for approved electronic encryption methods to communicate required information. The AFTAC SSO is the final authority for approval of contractor personnel SCI access. The COR will provide the SCI access nomination request form to the FSO/CSSOs, or CORs can accomplish.

3. The FSO/CSSO is responsible to establish and maintain an SCI personnel access list of those employees working on the contract to include sub-contractors FSO/CSSO will provide a copy of this list at least yearly to the PM/COR and SSO.

4. The FSO/CSSO will advise the PM and SSO immediately upon reassignment, dismissal, termination, or revocation of need-to-know for SCI cleared personnel on this contract. A formal notice to the SSO is required for processing debrief action. FSO/CSSOs will notify the PM and SSO immediately when there is a change in status of SCI indoctrinated contractor personnel IAW the security clearance adjudication guidelines identified in ICD 704.

5. FSO/CSSO must coordinate approval prior to subcontracting any portion of SCI efforts involved in the contract. The subcontractor DD Form 254 must have coordination signatures from the PM and SSO prior to administering.

6. Release of Information: Before releasing SCI information to a contractor facility, the COR will get approval from the SSO based on the work being performed.

7. SCI documentation, or other material concerning this contract will not be discussed with or released to any individual, subcontractor, agency (including Federal Government agencies and employees), and contractor employees not working on the contract without prior written approval from the PM.

8. Any SCI-derived material generated under this contract will be reviewed by the PM and SSO for proper classification prior to final publication and distribution. All non-SCI documents and publications developed by the contractor under this contract require mandatory review by the SSO and PM prior to public release authorization. Final Technical Reports must be sent to the SSO via approved shipping/handling methods at the address below.

9. Any SCI data released to or generated by the contractor in support of this contract remains the property of the DoD Department, agency, or command that released it. The contractor will maintain a record of all SCI released to contractor custody under this contract and upon completion/cancellation of the contract, must return all such material to the SSO. This applies to all data and materials, including working papers and notes. SCI data furnished to or generated by the contractor will require special security handling and controls beyond those in the National Industrial Security Program Operating Manual (NISPOM).

10. Access to SCI is limited to US Government locations identified under Block 8.a. or within a Government or Contractor approved SCI facility (SCIF) identified through an approved Memorandum of Agreement (MOA) or Co-Utilization Agreement (CUA). SCI level work may be approved at a contractor SCIF accredited by an agency other than DIA after CUA approval.

11. If this contract requires electronic processing of SCI, the PM must determine and request a SCIF requirement through the SSO in which DIA is the accrediting authority for AF sponsored SCIFs. Operational accreditation of AIS at the SCI level must be obtained through the ICD 503 A&A process.

12. This contract requires additional security requirements established for SCI in accordance with DoDM 5105.21, Volumes 1, 2, and 3; Intelligence Community Directives (ICD); ICD 503, ICD 704, ICD 705, and AFMAN 14-304.

13. The designated security management and oversight authority for SCI under this contract is:

SPECIAL SECURITY OFFICE
SSO Patrick
1020 South Patrick Drive
PAFB, FL 32925-3516

Phone: COMM: (321) 494-3427
DSN: 854-3427
SCI VOIP: 987-6252

JPAS SCI-SMO: **SSO Patric**

Hours of Operation: 0700-1630 Mon-Fri

PLA for M3 Messaging: **SSO PATRK**

Defense Courier Service (DCS) 3-Line Address:
416115-JA25 HKJ
184 NIP JA 023 023
SSO PATRICK

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION
EXTRACTED FROM DODM 5400.07_AFMAN 33-302 AND DODI 5200.48

1. CONTROLLED UNCLASSIFIED INFORMATION (CUI):

In addition to classified information, certain types of unclassified information also require application of access and distribution controls and protective measures for a variety of reasons. In accordance with Reference DoDI 5200.48, such information is referred to collectively as CUI. DoDI 5200.48 identifies the controls and protective measures developed for DoD CUI, Law Enforcement Sensitive (LES), DoD Unclassified Nuclear Information (DoD UCNI), and Limited Distribution) as well as some of those developed by other Executive Branch agencies.

2. CUI MARKINGS:

a. The CUI marking is assigned to information at the time of its creation by a DoD User Agency. It is not authorized as a substitute for a security classification marking, but is used on official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (FOIA) and an agency's Critical Information Indicators List (CIIL) referred to as OPSEC information.

b. Use of the above markings does not mean that the information cannot be released to the public, only that it must be reviewed by the Government prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.

3. IDENTIFICATION MARKINGS:

a. An unclassified document containing CUI will be marked "CUI" at the top and bottom of the front cover (if any), on the first page, on each page containing CUI, on the back page, and on the outside of the back cover (if any).

b. All DAF material containing CUI, including a document with comingled classified information, will include a CUI designation indicator IAW DoDI 5200.48, Figure 2. (Note: place in bottom right-hand corner of first page).

Controlled by: [Name of DoD Component] (Only if not on letterhead) Controlled by: [Name of Office] CUI Category: [List category or categories of CUI] Distribution/Dissemination Control:

c. Within a classified document, an individual page that contains CUI and classified information will be marked at the top and bottom with the highest security classification of information appearing on the page. If an individual portion contains CUI, but no classified information, the portion will be marked CUI.

d. Within a classified document, an individual page that contains CUI, but no classified information will be marked CUI at the top and bottom of the page, as well as each paragraph that contains CUI.

e. A warning box must be added to the first page of multi-page documents to alert readers to the presence of CUI in a classified DoD document.

This content is classified at the [insert highest classification level of the source data] level and may contain elements of controlled unclassified information (CUI), unclassified, or information classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer instead to [cite specific reference, where possible, or state "the applicable classification guide(s)"]. This content must be reviewed for both Classified National Security Information (CNSI) and CUI in accordance with DODI 5230.09 prior to public release. [Add a point of contact when needed.]

f. Any CUI released to a contractor by a DoD User Agency is required to be marked with the following statement prior to transfer:

This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA. Exemption(s) _____ applies/apply.

g. Removal of the CUI marking can only be accomplished by the originator or other competent authority. When the CUI status is terminated, all known holders will be notified to the extent practical.

4. **DISSEMINATION:** Contractors may disseminate CUI to their employees and subcontractors who have a need for the information in connection with a classified contract. Recipients shall be made aware of the status of such information, and transmission will be by means that preclude unauthorized public disclosure. Transmittal documents will call attention to the presence of CUI attachments.

5. **STORAGE:** During working hours, CUI shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During non-working hours, the information shall be stored to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks is adequate when internal building security is provided during non-working hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection of the material; can be stored in locked receptacles such as file cabinets, desks, or bookcases.

6. **TRANSPORTATION:** CUI may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail.

7. DISPOSITION & DISCLOSURE: When no longer needed, record copies of CUI may be disposed of by shredding. Unauthorized disclosure of CUI does not constitute a security violation, but the releasing agency must be informed of any unauthorized disclosure. Appropriate administrative action will be taken to fix responsibility for unauthorized disclosure whenever feasible, and appropriate disciplinary action will be taken against those responsible. The unauthorized disclosure of CUI protected by the Privacy Act may also result in civil and criminal sanctions.

a. The CUI marking is assigned to information at the time of its creation by a DoD User Agency. It is not authorized as a substitute for a security classification marking, but is used on official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (FOIA).

b. Use of the above markings does not mean that the information cannot be released to the public, only that it must be reviewed by the Government prior to its release to determine whether a significant and legitimate purpose is served by withholding the information or portions of it.

RELEASE OF NON-SENSITIVE COMPARTMENTED INFORMATION (NON-SCI) INTELLIGENCE INFORMATION TO US CONTRACTORS

1. Requirements for access to non-SCI intelligence:

a. All intelligence material released to the contractor remains the property of the US government and may be withdrawn at any time. Contractors must maintain accountability for all classified intelligence released into their custody.

b. The contractor must not reproduce intelligence material without the written permission of the originating agency through the Intelligence Support Office. If permission is granted, each copy shall be controlled in the same manner as the original.

c. The contractor must not destroy any intelligence material without advance approval or as specified by the Program Manager identified in Block 16 of the DD Form 254.

d. The contractor must restrict access to only those individuals who possess the necessary security clearance and who are actually providing services under the contract with a valid need-to-know. Further dissemination to other contractors, subcontractors, other government agencies, private individuals or organizations is prohibited unless authorized in writing by the originating agency through the Program Manager identified in Block 13 of the DD Form 254.

e. The contractor must ensure each employee having access to intelligence material is fully aware of the special security requirements for this material and shall maintain records in a manner that will permit the contractor to furnish, on demand, the names of individuals who have had access to this material in their custody.

f. Intelligence material must not be released to foreign nationals or immigrant aliens whether they are consultants, US contractors, or employees of the contractor and regardless of the level of their security clearance, except with advance written permission from the originator. Requests for release to foreign nationals shall be initially forwarded to the contract monitor and shall include:

(1) A copy of the proposed disclosure
(2) Full justification reflecting the benefits to US interests
(3) Name, nationality, particulars of clearance, and current access authorization of each proposed foreign national recipient

g. Upon completion or termination of the classified contract, or sooner when the purpose of the release has been served, the contractor will return all classified intelligence (furnished or generated) to the source from which received unless retention or other disposition instructions (see AFMAN 37-139) are authorized in writing by the Program Manager identified in Block 13 of the DD Form 254.

h. The contractor must designate an individual who is working on the contract as a custodian. The designated custodian shall be responsible for receipting and accounting for all classified material. The inner wrapper of all classified material dispatched should be marked to

the attention of a designated custodian and must not be opened by anyone not working directly on the contract.

i. Within 30 days after the final product is received and accepted by the procuring agency, classified intelligence materials released to or generated by the contractor, must be returned to the originating agency, through the Program Manager identified in Block 16 of the DD Form 254, unless written instructions authorizing destruction or retention are issued. Requests to retain material shall be directed to the Program Manager identified in Block 16 of the DD Form 254 for this contract in writing and clearly indicate the justification for retention and identity of the specific document to be retained.

j. Classification, regrading, or declassification markings of documentation produced by the contractor shall be consistent with that applied to the information or documentation from which the new document was prepared. If a compilation of information or a complete analysis of subject appears to require a security classification other than that of the source documentation, the contractor shall assign the tentative security classification and request instructions from the contract monitor. Pending final determination, the material shall be safeguarded as required for its assigned or proposed classification, whichever is higher, until the classification is changed or otherwise verified.

2. Intelligence material carries special markings. The following is a list of the authorized control markings of intelligence material:

a. "Dissemination and Extraction of Information Controlled by Originator (ORCON)." This marking is used, with a security classification, to enable a continuing knowledge and supervision by the originator of the use made of the information involved. This marking may be used on intelligence which clearly identifies, or would reasonably permit ready identification of an intelligence source or method which is particularly susceptible to countermeasures that would nullify or measurably reduce its effectiveness. This marking may not be used when an item or information will reasonably be protected by the use of other markings specified herein, or by the application of the "need-to-know" principle and the safeguarding procedures of the security classification system.

b. Authorized for Release to (Name of the Country(ies)/International Organization)." The above is abbreviated "REL_____." This marking must be used when it is necessary to identify classified intelligence material the US government originator has predetermined to be releasable or has been released through established foreign disclosure channels to the indicated country(ies) or organization.

3. The following procedures govern the use of control markings:

a. Any recipient desiring to use intelligence in a manner contrary to restrictions established by the control markings set forth above shall obtain the advance permission of the originating agency through the Program Manager identified in Block 16 of the DD Form 254. Such permission applies only to the specific purposes agreed to by the originator and does not automatically apply to all recipients. Originators shall ensure that prompt consideration is given to recipients' requests in these regards, with particular attention to reviewing and editing, if

necessary, sanitized or paraphrased versions to derive a text suitable for release subject to lesser or no control markings.

b. The control marking authorized above shall be marked on the title page, front cover, and other applicable pages of documents, incorporated in the text of electrical communications, marked on graphics, and associated (in full or abbreviated form), data stored or processed in automatic data processing systems. The control marking also shall be indicated by parenthetical use of the marking abbreviations at the beginning or end of the appropriate portions. If the control marking applies to several or all portions, the document must be marked with a statement to this effect rather than marking each portion individually.

c. The control markings shall be individually assigned at the time of preparation of products and used in conjunction with security classifications and other markings specified by Executive Order (E.O.) 13526 and its implementing security directives, in addition to previous E.Os. The marking shall be carried forward to any new format in which the same information is incorporated including oral and visual presentations.

4. Request for release of intelligence material to a contractor not working on an AFTAC contract, must be prepared by the Program Manager identified in Block 16 of the DD Form 254 and submitted through the AFTAC SO as designated in Block 15 of the DD Form 254. This should be accomplished as soon as possible after the contract has been awarded. The request must include a copy of the DD Form 254 and the Statement of Work.

10.b,c,d: Government Contracting Agency (GCS) approval is required prior to granting CNWIDI to a subcontractor. The Secretary of Energy and the Chairman of the Nuclear Regulatory Commission retain authority over access to information that is under their respective cognizance as directed by the Atomic Energy Act of 1954. The Secretary of Energy may inspect and monitor contractor programs or facilities that involve access to such information or may enter written agreement with the DoD to inspect and monitor these programs or facilities. A special briefing is required for access to CNWDI, and a final security clearance is required for access to CNWDI and RD information. Only contractors approved by the AFTAC RD Manager may classify RD and FRD documents.

10.e.: (1): All Intelligence Information required for this contract will be handled in accordance with special security requirements provided in Attachment: 'ACCESS TO SENSITIVE COMPARTMENTED INFORMATION,' and regulations listed in Items 13 and 14."

10.e.(2): Access to intelligence information will be handled in accordance with Attachment entitled 'Release of Non-SCI Intelligence Information to U.S. Contractors.'"

10.g: A NATO awareness briefing must be accomplished before access to SPIRNET/JWICS computer system is granted.

10.j.: Controlled Unclassified Information provided under this contract shall be safeguarded as specified in the Attachment, 'Protecting Controlled Unclassified Information.'"

ITEM 11:

11.c: The contractor requires access classified source data up to and including SECRET in support of the work effort. (If FRD, RD, or CNWIDI information is going to be stored or worked on at the contactor facility add to this line.)

11.h: 11.h. REQUIRE A COMSEC ACCOUNT: This block is checked if the contractor requires a COMSEC account at the contractor location in support of a DCSA accredited "open" or "closed" area used for processing classified material.

11.i: See AFTAC/SO for statement

Ref Item 14: SSO Patrick, 1020 South Patrick Drive Building 10989, PSFB, FL 32925 (321) 494-2836

Ref Item 15: ISPM SSO Patrick, 1020 South Patrick Drive Building 10989, PSFB, FL 32925 (321) 494-2836

Ref Item 15: Industrial Security Reviews: Will be conducted by the ISPM while operating on an Air Force Installation.

Level of Access Required: TS/SI/TK/GG/HCS