



DEPARTMENT OF THE NAVY  
COMMANDER NAVY RESERVE FORCE  
1915 FORRESTAL DRIVE  
NORFOLK VA 23551-4615

COMNAVRESFORINST 4200.35A  
N4  
10 Feb 25

COMNAVRESFOR INSTRUCTION 4200.35A

From: Commander, Navy Reserve Force

Subj: SENSITIVE ACTIVITY AND INTELLIGENCE-RELATED CONTRACTING  
WITHIN THE NAVY RESERVE FORCE

Ref: (a) SECNAVINST S4200.35A  
(b) DoD Directive 5148.13  
(c) DoD Instruction O-5100.94  
(d) DoD Manual 5105.21  
(e) COMNAVRESFORINST 5510.9A  
(f) COMNAVRESFOR Reserve Force SSO Designation Letter  
(g) Federal Acquisition Regulation (FAR) Part 2.101  
(h) DoD 5220.22-M  
(i) Federal Acquisition Regulation (FAR) Subpart 4.8 Government Contract Files –  
28 October 2022  
(j) SECNAV Manual 5210.1  
(k) OPNAVINST 5215.17A  
(l) SECNAVINST S5410.4B  
(m) SECNAVINST 5000.34G  
(n) SECNAVINST S5410.4B

Encl: (1) Definitions  
(2) Activity internal SAIRC Flow Chart  
(3) Initial Screening Questionnaire  
(4) SAIRC Detailed Screening  
(5) Activity SAIRC-RB Negative Determination Notification Example  
(6) SAIRC Determination Letter Example  
(7) Certification of Classification Memo Example  
(8) SAIRC Designation Letter Example  
(9) Activity SAIRC Report  
(10) DD Form 254, DoD Contract Security Classification Specification  
(11) DD Form 254, SCI Addendum Template  
(12) Complete Package Checklist

1. Purpose. Establishes policy, procedures, and responsibilities for the review of acquisition packages to identify and validate presence of one or more Sensitive Activity and Intelligence Related Contracting (SAIRC) criteria, and the administrative handling of any package that requires SAIRC support via SAIRC Review Board (SAIRC-RB) processing in accordance with references (a) through (n).

2. Cancellation. COMNAVRESFORINST 4200.35

10 Feb 25

3. Background. References (a) through (n) provide the regulatory basis of sensitive activity and intelligence related acquisition package management. The SAIRC program is designed to stop, deter, and avoid the continued practice of “gray contracting.” A gray contract fails to clearly describe the complete or true nature of the effort required by the government, typically in order to avoid administrative security procedures. Gray contracts hide sensitive or classified activities in non-sensitive or unclassified contracts with the intention of circumventing proper legal prerogatives and oversight responsibilities. Gray contracting puts Department of Navy (DON) programs and the DON itself at risk by not allowing the government to hold the performer accountable. The SAIRC process provides appropriate protection measures for contracts supporting classified or sensitive activities and operations. This instruction implements the policy and procedures of reference (a) within Commander, Navy Reserve Force (COMNAVRESFOR) and all subordinate commands.

4. Applicability. This instruction applies to all contractual requirements in support of COMNAVRESFOR and subordinate commands including those that are funded by a request for contractual procurement (NAVCOMPT 2276), Military Interdepartmental Purchase Request (MIPR), project, work order, or any other method for obtaining contractor support.

a. SAIRC does NOT apply to:

(1) Approved Special Access Programs (SAP).

(2) Intelligence and/or sensitive activities approved through the Defense Sensitive Support (DSS).

(3) Intelligence and/or sensitive activities within the scope of existing DON approved Memorandum of Understanding.

(4) Administrative actions such as changes in funding or purchase amounts that do not change/modify the Performance Work Statement (PWS), Statement of Work (SOW), or Specifications. (Changes in purchase type (e.g. brand, model, etc.) require a new screening.)

## 5. Policy

a. COMNAVRESFOR requests for SAIRC support must be validated with a signature by COMNAVRESFOR. All subordinate command (echelon III and below) requests for SAIRC support must be validated by signature approval from Deputy Commander, Navy Reserve Force. Per reference (a) paragraph 6d, delegation of these signature approval authorities is not authorized for those contracting action candidate packages determined to meet SAIRC criteria by the sponsoring command’s self-screen.

b. Classified and unclassified contracts should be screened against SAIRC criteria because the classification does not preclude it from SAIRC review. Per reference (e), all acquisition packages must be initially reviewed by the Requirements Owner to screen against the SAIRC criteria to determine SAIRC applicability as defined in reference (a) enclosure (2), paragraph 9.

10 Feb 25

## 6. Responsibilities

### a. DON SAIRC Review Board (DON SAIRC-RB)

- (1) Provide equity and risk assessment review on all SAIRC submission packages for the DON.
- (2) Administer the DON SAIRC program.
- (3) Make final determination whether proposed contracting actions meet criteria for additional protections.
- (4) Provide adjudication results of SAIRC submission packages within 30 calendar days of receipt.
- (5) Composed of representatives from the following offices:
  - (a) Deputy Under Secretary of the Navy for Intelligence and Security.
  - (b) Assistant Secretary of the Navy, Research Development and Acquisition.
  - (c) Director of National Intelligence.
  - (d) U.S. Marine Corps Director of Intelligence.
  - (e) Department of the Navy Special Access Program Central Office.
  - (f) Department of the Navy Office of General Counsel.

### b. DON SAIRC Review Board Executive Secretary (DON SAIRC-RB ExSec).

- (1) The sole point of entry for new SAIRC submission packages.
- (2) Verify completeness of SAIRC Submission Packages.
- (3) Refer SAIRC submission packages to the DON SAIRC-RB.
- (4) Notify requesting activity of DON SAIRC-RB adjudication results.
- (5) Transmit SAIRC-RB approved packages for work assignment.
- (6) Maintain metrics on process efficiency and performance.

### c. Requesting DON Activity Commander.

- (1) Validate all requests for support via signature approval O-7 and above or civilian equivalent for all contracts that meet SAIRC criteria. This authority may not be delegated.

10 Feb 25

(2) Nominate appropriately cleared Requirement Owners and/or Program Managers with requisite training to coordinate with Collateral or Sensitive Compartmented Information (SCI) Industrial Security Officers as appropriate.

d. Requesting Activity.

- (1) Designate in writing an appropriately cleared activity SAIRC Officer.
- (2) Ensure all contracting actions requirements are screened against SAIRC criteria.
- (3) Create a known, repeatable, and auditable process to screen contracts.
- (4) Hold a monthly SAIRC review board as needed.

e. Activity SAIRC Review Board (SAIRC-RB).

(1) Screen all contracts that meet SAIRC criteria via the Initial SAIRC Questionnaire. The board will be composed of the following members at a minimum:

- (a) Activity SAIRC Officer.
- (b) Activity Contractual Services Manager.
- (c) Requirement Owner or Subject Matter Expert.
- (d) Intelligence Officer.
- (e) Industrial Security Representative.
- (f) Legal Representative.

- (2) Determine risk assessment as outlined in reference (a).
- (3) Author risk criteria and rationale for the SAIRC determination letter (Enclosure (6)).

f. Activity SAIRC Officer (SAIRCO).

- (1) Designated in writing (Enclosure (8)).
- (2) Chair the activity SAIRC-RB and document all decisions.
- (3) Have appropriate expertise to assume risk.
- (4) Recommend contracts for additional screening to the SAIRC-RB as appropriate.
- (5) Ensure SAIRC submission packages are appropriately classified.

10 Feb 25

(6) Provide training to the Activity Contractual Services Manager, all Requirement Owners, and SAIRC-RB members.

(7) Submit positively screened SAIRC contracts to the DON SAIRC-RB ExSec via the Activity Commander using the SAIRC submission package format.

g. Activity Contractual Services Manager.

(1) Verify all contacting actions (except those listed in paragraph 3.a) include a SAIRC screening determination.

(2) Serve on the SAIRC-RB as contracting Subject Matter Expert (SME).

h. Requirements Owner.

(1) Verify the Statement of Work (SOW) or Performance Work Statement (PWS) capture all details of the requested work.

(2) Ensure strict compliance with the contract terms and conditions.

(3) Conduct Initial SAIRC Screening via Initial Screening Questionnaire (Enclosure (3)).

(4) Forward any positive initial SAIRC screenings to the activity SAIRCO.

(5) Serve on the SAIRC-RB for owned contracts to answer questions about the scope of requested work.

i. Intelligence Officer.

(1) Serve on the SAIRC-RB as intelligence related activity SME.

(2) Serve as translator to the board for intelligence specific terms.

(3) Provide determination on whether contracting action meets intelligence criteria.

(4) Verify any intelligence related activity is adequately defined in the SOW and PWS.

(5) May be the same person as the SAIRCO.

(6) An Operations Office may be used for non-Intelligence Activities.

j. Industrial Security Officer (ISO).

(1) Applicable to Collateral and SCI Industrial Security Officers as needed.

(2) Review SOW and PWS for proper clearance requirements.

10 Feb 25

(3) Verify clearance requirements do not exceed the requested work. (Elevated security requirements are not authorized for “future operations”).)

(4) Serve on the SAIRC-RB as the Security SME.

k. Legal Representative.

(1) Serve on the SAIRC-RB as the legal SME.

(2) Ensure compliance with existing legal statutes, regulations directives and policy.

(3) Verify oversight authority.

l. Information Security Officer.

(1) Applicable to Collateral and SCI Information Security Officers as needed.

(2) Review SAIRC Submission Packages as required for proper markings.

(3) Per references (h) and (i), provide an SCI addendum to the DD Form 254 if the package meets the SAIRC criteria for SCI caveats and controls. The SCI addendum will describe access to SCI information, governing policies, and where the SCI work will be conducted (template Enclosure (11)).

m. Personnel Security Officer (PSO).

(1) Verify SAIRC-RB members are authorized access to the appropriate classification level for each SAIRC review (e.g. Secret, Top Secret, SCI, SAP).

(2) Applicable to Collateral and SCI Personnel Security Officers, as needed.

(3) Verify Need-to-Know requirements and enter access allowances in the Defense Information System for Security (DISS).

(4) Facilitate contractor/sub-contractor access to classified material, if warranted.

6. Action. The SAIRC-RB will meet at least monthly, to review all contracts that receive positive SAIRC initial screenings as determined by the Requirements Owner and SAIRCO. Meetings may be deferred if no contracting actions require screening beyond the initial questionnaire.

a. Initial Screening Questionnaire. **The Initial Screening Questionnaire (Enclosure (3)) will be completed by the Requirements Owner.** If the initial screening meets SAIRC criteria, the contract will be verified by the Activity SAIRCO and referred to the SAIRC-RB for detailed review if needed. A new SAIRC initial screening will be conducted any time the contract requirements are modified.

(1) The Initial Screening Questionnaire will include the following questions:

10 Feb 25

(a) Is any portion of the requested work description or supporting documents classified?

(b) Does the Statement of Work and any associated supporting documents as written or defined omit significant elements of the requested work in order to remain unclassified, or lower the overall classification of the contract package?

(c) Does the requested requirement description and any associated supporting documents as written or described reveal, or potentially reveal, an Intelligence Activity, Sensitive Activity, or Sensitive Operation per SECNAVINST 5000.34 (series)?

(d) Is there any portion of the requested work description and any associated supporting documents that cannot, or should not, be published openly to the public?

**If the answer to all of the questions is "No", the completed Initial Screening Questionnaire will be placed in the Contract File and the contracting process can continue.**

**If the answer to any of these questions is "Yes", the contract must be referred to the SAIRC-RB for additional screening.**

b. Detailed SAIRC Screening. The Detailed SAIRC Screening (Enclosure (4)) will be completed by the SAIRC-RB. For contracts that receive a positive SAIRC screening by the SAIRC-RB, a SAIRC Submission Package will be generated and routed to the Activity Commander for signature and referred to the DON SAIRC-RM ExSec via SSO Navy for review based on classification level:

(1) SIPR (SAIRC-RB\_Executive\_Secretary@navy.smil.mil)

(2) JWICS (SAIRC-RB\_Executive\_Secretary@nmic.ic.gov)

Negative screenings will be announced to the Requirements Owner via unclassified memoranda (Encl (5)). Any notes resulting from the SAIRC-RB will be collected by the SAIRCO following the review and filed with the Detailed SAIRC Screening.

(3) The SAIRC Submission Package will include the following:

(a) SAIRC Determination Letter (Enclosure (6)), signed by the Activity Commander (O-7 and above or SES equivalent), which will include:

1. Authority to perform contracting action.

2. Identification of SAIRC criteria and rationale.

3. Risk Assessment.

(b) Certification of Classification Memorandum (Enclosure (7)).

(c) DD Form 254 and SCI Addendum (if required (Enclosure (10) and (11))).

10 Feb 25

- (d) A complete and accurate SOW/PWS or requirement description.
- (e) Detailed SAIRC screening completed by the [Activity] SAIRC-RB (Enclosure (4)).
- (f) Other supporting documents as applicable.

c. DON SAIRC-RB Determinations and Outcomes.

(1) There are four (4) critical determinations evaluated by the DON SAIRC-RB:

- (a) Is this a valid contract?
- (b) Is the requirement within the Activity's scope of authority to request?
- (c) Risk Assessment:
  - 1. Does the requirement meet the elevated risk threshold? (See paragraph 6.d)
  - 2. What is the exposure of the activity?
  - 3. What is the risk of the contracting action?
  - 4. Are risks properly identified, mitigatable, and deemed acceptable?
  - 5. What is the proposed gain/probability of that outcome?

(d) Does the requirement merit additional protections per reference (a)?

(2) There are three (3) potential outcomes from the DON SAIRC-RB screening:

- (a) Forward to appropriate activity for contracting action.
- (b) Return to requesting activity for local contracting action.
- (c) All Stop:
  - 1. Not a valid requirement.
  - 2. Residual risk is unacceptable.
  - 3. Request is bypassing other established processes (e.g., DSS, SAPCO).

d. Risk Thresholds. The Deputy Under Secretary of the Navy for Intelligence and Security has the final validation approval for SAIRC submission packages where it is determined that the risk assessment meets elevated risk criteria as outlined in reference (a).



10 Feb 25

(1) Likelihood + consequence = elevated risk

(2) Elevated risk is defined as  $\geq 50\%$  likely to cause one or more of the following:

(a) Serious Damage to National Security;

(b) Serious public controversy and/or embarrassment to the United States, Department of Defense, or Department of the Navy;

(c) Severe injury or permanent partial disability;

(d) Extensive damage to equipment or systems;

(e) Significant damage to property or equipment;

(f) Security failure;

(g) Significant collateral damage; or

(h) Significant adverse impact on foreign military and/or diplomatic relations.

#### 8. Reporting

a. Each Echelon III activity is required to submit an annual SAIRC report to the Force SAIRCO which can be found in Encl (9). Reports will be retained by Activity and Force SAIRCOs for a period of five (5) years and will be made available for inspection when requested.

b. This report will include the following:

(1) Number of unclassified and classified contract requirements submitted by the command. This is specific to contracted requirements requested by the activity itself and does not include any contracts processed for down echelon activity.

(2) Number of SAIRC initial screenings forwarded to the SAIRCO.

(3) Number of positive SAIRC initial screenings.

(4) Number of times the Activity SAIRC-RB was convened.

(5) Number of packages submitted to the DON SAIRC-RB.

(6) SAIRCO POC information.

c. Echelon III SAIRCOs may require lower echelon activities to consolidate final reports, but must still collect and retain all lower echelon reports.

9. Retention. SAIRC screenings will be retained with contract files in accordance with reference (i).

10. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per reference (j).

11. Review and Effective Date. Per Reference (k), COMNAVRESFOR N4 will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, Navy policy and regulatory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 10 years after effective date unless reissued or canceled prior to the 10-year anniversary date, or an extension has been granted.



M. J. STEFFEN  
Deputy Commander

10 Feb 25

### Definitions

Contract - Any type of agreement or order for the procurement of goods and services.

Contracting Action - Any oral or written action that results in the purchase, rent, or lease of supplies or equipment, services, or construction using appropriated dollars over the micro-purchase threshold, or modifications to these actions regardless of dollar value.

Government Contract File - Record of all contractual actions. Must be sufficient to constitute a complete history of the transaction.

Intelligence-Related Activity - Activities not conducted under the authority of E.O. 12333 that involve the collection, retention, or analysis of information, and the activity's primary purpose is to:

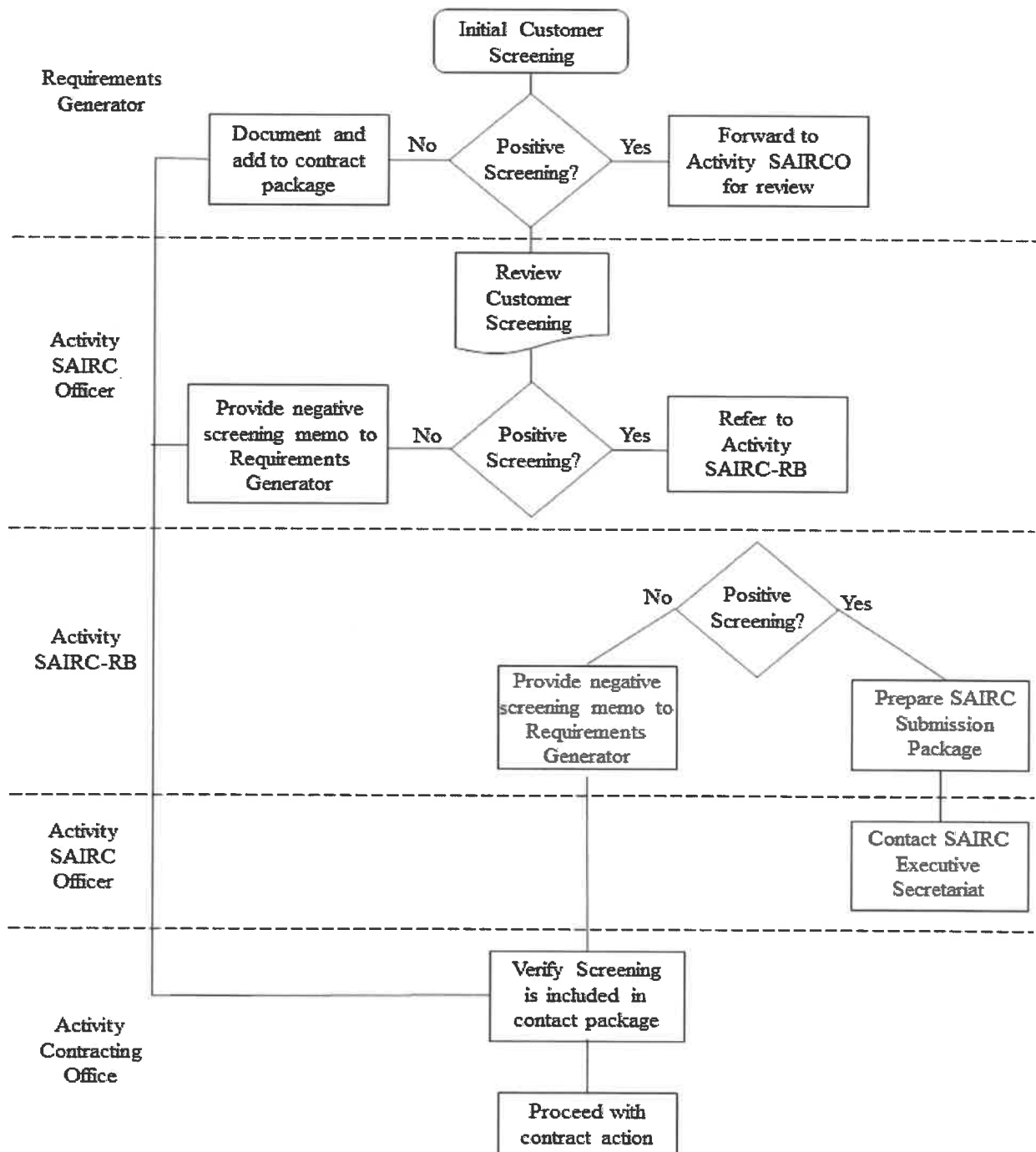
- Train intelligence personnel
- Conduct research, development, or testing and evaluation of developing intelligence-specific capabilities.
  - Activities that use intelligence funding are presumed to be intelligence or intelligence-related.
  - Excluded activities include, but are not limited to:
    - Operational Security activities, such as own force monitoring.
    - Force Protection.
    - Maintenance of technologies or systems.
    - Cyberspace surveillance and reconnaissance operations.
    - Activities defined in DoDM 5240.01 support activities.

Sensitive Activities - Operations, actions, activities, or programs that are generally handled through special access, compartmented, or other sensitive control mechanisms because of the nature of the target, the area of operation, or other designated aspects. This includes operations, actions, activities, or programs supported by any DoD component that, if compromised, could have enduring adverse effects on U.S. foreign policy, DoD or DON activities, or military operations; or cause significant embarrassment to the United States. Sensitive Activities include, but are not limited to:

- Intelligence Activities, Related Activities, and Related Contracting
- DSS
- Cover
- SAPs
- Activities covered under ACCMs

This includes contracting actions which may reveal sensitive activities or operations.

Activity Internal SAIRC Flow Chart



**Initial Screening Questionnaire**

DATE: [DD MMM YY]

MEMORANDUM

From: [COR]  
To: [SAIRCO]

Subj: INITIAL CUSTOMER SCREENING QUESTIONNAIRE FOR S4200.35 (SERIES)  
COMPLIANCE ISO CONTRACT [Contract Number]

Ref: (a) SECNAVINST S4200.35A  
(b) CNRFINST 4200.35A

Encl: (1) Contract Package

1. The Initial SAIRC Screening Questionnaire is used to evaluate contracting actions to ensure they do not inadvertently qualify for SAIRC.
2. "Yes" answers require additional review by the Activity SAIRCO.
  - a. Is any portion of the work description or supporting documents classified (U) Does the Statement of Work and any associated supporting documents as written or defined omit significant elements of the requested work in order to remain unclassified, or lower the overall classification of the contract package
  - b. Does the requested requirement description and any associated supporting documents as written or described reveal, or potentially reveal, an Intelligence Activity, Sensitive Activity, or Sensitive Operation per SECNAVINST 5000.34 (series)?
  - c. Is there any portion of the requested work description and any associated supporting documents that cannot, or should not, be published openly to the public?
3. It has been determined that this requirement has been properly screened; and
4. The below signature identifies and validates the contract's initial review has determined that the contracting action [requires/does not require] additional screening.

---

Contract Office Representative (COR)

**SAIRC Detailed Screening**

(Ensure proper classification markings as required)

DATE: [DD MMM YY]

MEMORANDUM

From: [Activity SAIRC-RB]

To: [Activity SAIRCO]

Subj: [Activity] REVIEW BOARD SCREENING FOR S4200.35 (SERIES) COMPLIANCE  
ISO CONTRACT [Contract Number]

Ref: (a) SECNAVINST S4200.35A  
(b) CNRFINST 4200.35A

Encl: (1) Contract Package

1. Each question is to be carefully reviewed by the [Activity] SAIRC Review Board. Questions should be answered in detail at the lowest security level possible while maintaining informative accuracy for risk determination. Annotate separate answers as needed for each SAIRC criteria met.

2. The requesting COR will be notified by the SAIRC-RB within 5 business days of negative screenings via a memo for inclusion in the contracting package.

- a. What is the classification requirement of the contract?
- b. How many contract personnel will be required to fulfill this requirement? (Enter N/A if procurement or acquisition contract)
- c. Briefly describe how the requested service meets SAIRC criteria.
- d. Briefly describe the purpose or goal of the requested service.
- e. Is this requirement at the behest of the Intelligence Community?
- f. Describe why this service is unable to be accomplished using existing federal channels or employees.
- g. Is there a non-contracting way to accomplish the requested service?
- h. Does the requesting activity have the authority to request this service?
- i. Does the service require the performance of Intelligence-related activities?
- j. Does the service require the performance of clandestine trade work or operations?
- k. Does the service work require "cover"?

Enclosure (4)

10 Feb 25

[Activity] REVIEW BOARD SCREENING FOR S4200.35 (SERIES) COMPLIANCE ISO  
CONTRACT [Contract Number]

1. Does the service require/allow non-DoD personnel to act on behalf of the DoD?
  - m. Does this service require/allow activities to be undertaken in a partner nation or leveraging a partner nation's assets, without that nation's knowledge?
  - n. What risk is assumed if the contracting action is not approved?
  - o. Identify the risks associated with the contract:
    - (1) Could exposure of this service cause damage to National Security? If so, at what level (Serious, Grave, Exceptionally Grave, etc)?
    - (2) Could exposure of this service cause embarrassment to the United States, Department of Defense, or Department of the Navy?
    - (3) Could exposure of this service result in severe injury or permanent partial disability of the contractors or other personnel? (Other personnel is not limited to U.S. persons.)
    - (4) Could this service result in extensive damage to equipment or systems?
    - (5) Could this service result in significant damage to property?
    - (6) Could exposure of this service expose failures in security?
    - (7) Could this service result in significant collateral damage?
    - (8) Could exposure of this service have a significant adverse impact on foreign military and/or diplomatic relations?
  - p. Are the risks associated with this contract able to be mitigated? If so, describe how.
  - q. Are the mitigations realistic, inspectable, and acceptable?
  - r. Do risk mitigations require services from outside the requesting activity? If so, what other activities would be involved? List the activities and their degree of involvement.
  - s. Do Memoranda of Understanding/Agreements exist between the requesting activity and activities supporting risk mitigations? (Provide copies).
2. [(U)/(CUI)] It has been determined that this requirement has been properly screened; and the contracting action [Does/Does Not] require submission to the SAIRC Executive Secretariat.
3. (U) The below signatures identify the screeners and validates the [Activity] SAIRC-RB results.

[*Activity*] REVIEW BOARD SCREENING FOR S4200.35 (SERIES) COMPLIANCE ISO  
CONTRACT [*Contract Number*]

SAIRCO:	<hr/>	<hr/>
	Print Name	Signature
COR:	<hr/>	<hr/>
	Print Name	Signature
SME:	<hr/>	<hr/>
	Print Name	Signature
Intelligence:	<hr/>	<hr/>
	Print Name	Signature
Security:	<hr/>	<hr/>
	Print Name	Signature
Legal:	<hr/>	<hr/>
	Print Name	Signature

Copy to: SAIRC Executive Secretariat via Submission Package



**Activity SAIRC-RB Negative Determination Notification Example**

DATE: [DD MMM YY]

MEMORANDUM

From: [Activity] SAIRC Review Board –OR- SAIRCO

To: [COR]

Subj: (RESULTS OF [ACTIVITY] SAIRC REVIEW FOR S4200.35 (SERIES)  
COMPLIANCE ISO CONTRACT [Contract Number]

Ref: (a) SECNAVINST S4200.35A  
(b) CNRFINST 4200.35A  
(c) DETAILED SAIRC SCREENING [date]

1 A detailed review of this contract has determined that the requested contracting action **DOES NOT** meet SAIRC criteria. The contracting action may proceed.

2 This memo will be submitted with the contract package and will be retained by the Contracting Office with the associated contract files for this contract. Ref (c) will be maintained by the [Activity] SAIRC Officer for the life of the contract or [declassification date], whichever occurs last.

3 Questions about this determination can be directed to the [Activity] SAIRC Officer at xxx-xxx-xxxx or via e-mail at xxxxx.x.xxxxx.xxx@us.navy.mil.

FIRSTNAME LASTNAME  
Chair, [Activity] SAIRC-RB

10 Feb 25

**SAIRC Determination Letter Example**

(Activity letterhead required)

(Classify as Appropriate)

SER ##

DD MMM YY

MEMORANDUM FOR THE RECORD

From: [Activity Commander (O-7 and above or SES)]

To: Sensitive Activities & Intelligence Related Contracting Review Board

Subj: SAIRC CRITERIA DETERMINATION

Ref: (a) SECNAVINST S4200.35A

Encl: (1) SAIRC SUBMISSION PACKAGE ISO CONTRACT [Contract number]

1 In accordance with Ref (a), [Requesting Activity] submits the attached package for Sensitive Activities Classified Contracting Review Board (SAIRC-RB) consideration.

2 [(Class)] This contracting action is in direct support of [requirement] and has been validated by [e.g. JROCM, UON (JUON or JUEN)] or is in alignment with [e.g. NDS, NDAA, USD (R&E), SECNAV or CNO priorities].

3 This contracting action is within [Requesting Activity]'s Scope of Authority.

4 [(Class)] This contracting action meets the following SAIRC Screening Criteria:

a. [Criteria and rationale]

b. [Criteria and rationale]

5 [(Class)] This contracting action [meets/does not meet] the elevated DON risk thresholds.

6 My POC on this matter is [SAIRCO Name] who may be contacted at [phone] or via e-mail at [e-mail].

F. M. LASTNAME

Enclosure (6)

10 Feb 25

**Certification of Classification Example**

DD MMM YY

MEMORANDUM FOR THE RECORD

From: [Activity Special Security Officer or Information Security Officer]  
To: Sensitive Activities & Intelligence Related Contracting (SAIRC) Executive Secretariat  
Via: [Activity] SAIRC Officer

Subj: CERTIFICATION OF CLASSIFICATION ISO CONTRACT [Contract Number]

Ref: (a) SECNAVINST S4200.35A  
(b) [Applicable Security Classification Guide]

Encl: (1) SAIRC Submission Package

1. (U) In accordance with Ref (a), I hereby certified that Encl (1) has been reviewed against the security classification guidelines laid out in Ref (b).
2. (U) It has been determined this submission package meets classification requirements and has been properly marked.
3. (U) The derivative classifier information for this submission package is identified below:
  - a. Name: [First MI Last]
  - b. Rank/Rate/Paygrade:
  - c. Contact: [Phone and e-mail]
  - d. Derivative Classification Training Completed on: [Date]
4. (U) Please direct questions concerning this classification review to [Reviewer name] at [phone] or via e-mail at [e-mail].

FIRSTNAME LAST NAME  
[Activity] [Special/Information] Security Officer

10 Feb 25

**SAIRC Designation Letter Example**

(Activity letterhead required)

5500  
SER: ##  
DD MMM YY

From: [Activity Commander]

To: [Rank, Full Name]

Subj: DESIGNATION AS SENSITIVE ACTIVITIES AND CLASSIFIED CONTRACTING  
(SAIRC) OFFICER FOR [ACTIVITY]

Ref: (a) CNRFINST 4200.35A

1. Per reference (a), you are hereby designated as the Sensitive Activities and Classified Contracting (SAIRC) Officer for [Activity]. You are responsible for managing the SAIRC program and chairing the Activity SAIRC Review Board. The following information is provided for contact and liaison purposes:

a NAME: [First MI Last]

b RATE/RANK/PAYGRADE:

c DoDID:

d UIC:

e PHONE:

f E-MAIL:

2. You are directed to become thoroughly familiar with Ref (a), and all additional references identified therein, in carrying out your assigned duties.

3. Your appointment will remain in effect until such time that you are relieved of your responsibilities by a competent authority.

F.M. LASTNAME

Copy to:  
SAIRC-RB Executive Secretariat

Enclosure (8)

10 Feb 25

(Activity letterhead required)

**Activity SAIRC Report**

5500

SER: ##

DD MMM YY

From: [Activity SAIRCO]

To: [ISIC SAIRCO]

Subj: ANNUAL SENSITIVE ACTIVITIES AND INTELLIGENCE RELATED  
CONTRACTS REPORT FOR [YEAR]

Ref: (a) (U) CNRFINST 4200.35A

1. Per Ref (a), the following Sensitive Activities and Intelligence Related Contacts (SAIRC) actions and reviews occurred for [Activity] from October 1, [Year] to September 30, [Year]:

a Number of Contract Requirements submitted

(1) Unclassified:

(2) Classified:

b Number of Initial SAIRC Screenings forwarded to the SAIRCO:

c Number of Positive Initial SAIRC Screenings:

d Number of Times Activity SAIRC-RB convened:

e Number of Packages submitted to the DON SAIRC-RB, Executive Secretariat:

2. Please direct questions concerning this report to the [Activity] SAIRCO, [Name] at [phone] or via e-mail at [e-mail].

F.M. LASTNAME  
[Activity] SAIRCO

Enclosure (9)

<b>CLASSIFICATION (When filled in):</b> <span style="border: 1px solid black; padding: 2px;"> </span>	
<b>DEPARTMENT OF DEFENSE</b> <b>CONTRACT SECURITY CLASSIFICATION SPECIFICATION</b> <i>(The requirements of the National Industrial Security Program (NISP) apply to all security aspects of this effort involving classified information.)</i>	
OMB No. 0704-0567 OMB approval expires: May 31, 2022	
<p>The public reporting burden for this collection of information, 0704-0567, is estimated to average 70 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Washington Headquarters Services, at <a href="mailto:whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil">whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil</a>. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p style="text-align: center;"><b>RETURN COMPLETED FORM AS DIRECTED IN THE INSTRUCTIONS.</b></p>	
<b>1. CLEARANCE AND SAFEGUARDING</b>	
<b>a. LEVEL OF FACILITY SECURITY CLEARANCE (FCL) REQUIRED</b> <i>(See instructions)</i> <div style="border: 1px solid black; height: 20px; margin-top: 5px;"></div>	<b>b. LEVEL OF SAFEGUARDING FOR CLASSIFIED INFORMATION/ MATERIAL REQUIRED AT CONTRACTOR FACILITY</b> <div style="border: 1px solid black; height: 20px; margin-top: 5px;"></div>
<b>2. THIS SPECIFICATION IS FOR:</b> <i>(X and complete as applicable.)</i>	
<input type="checkbox"/> <b>a. PRIME CONTRACT NUMBER</b> <i>(See instructions.)</i> <div style="border: 1px solid black; height: 20px; margin-top: 5px;"></div> <input type="checkbox"/> <b>b. SUBCONTRACT NUMBER</b> <div style="border: 1px solid black; height: 20px; margin-top: 5px;"></div> <input type="checkbox"/> <b>c. SOLICITATION OR OTHER NUMBER</b> <b>DUE DATE (YYYYMMDD)</b> <div style="border: 1px solid black; height: 20px; margin-top: 5px;"></div>	<b>3. THIS SPECIFICATION IS:</b> <i>(X and complete as applicable.)</i>
<input type="checkbox"/> <b>a. ORIGINAL</b> <i>(Complete date in all cases)</i> <b>DATE (YYYYMMDD)</b> <div style="border: 1px solid black; height: 20px; margin-top: 5px;"></div> <input type="checkbox"/> <b>b. REVISED</b> <i>(Supersedes all previous specifications)</i> <b>REVISION NO.</b> <b>DATE (YYYYMMDD)</b> <div style="border: 1px solid black; height: 20px; margin-top: 5px;"></div> <input type="checkbox"/> <b>c. FINAL</b> <i>(Complete Item 5 in all cases)</i> <b>DATE (YYYYMMDD)</b> <div style="border: 1px solid black; height: 20px; margin-top: 5px;"></div>	
<b>4. IS THIS A FOLLOW-ON CONTRACT?</b> <input type="checkbox"/> No <input type="checkbox"/> Yes <i>If yes, complete the following:</i> Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.	
<b>5. IS THIS A FINAL DD FORM 254?</b> <input type="checkbox"/> No <input type="checkbox"/> Yes <i>If yes, complete the following:</i> In response to the contractor's request dated _____, retention of the classified material is authorized for the period of: _____	
<b>6. CONTRACTOR</b> <i>(Include Commercial and Government Entity (CAGE) Code)</i>	
<b>a. NAME, ADDRESS, AND ZIP CODE</b> <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>	<b>b. CAGE CODE</b> <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>
<b>c. COGNIZANT SECURITY OFFICE(S) (CSO)</b> <i>(Name, Address, ZIP Code, Telephone required; Email Address optional)</i> <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>	
<b>7. SUBCONTRACTOR(S)</b> <i>(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)</i>	
<div style="display: flex; justify-content: flex-end; gap: 10px;"> <span>Add Row</span> <span>Remove last Row</span> <span>Delete All Rows</span> </div>	
<b>a. NAME, ADDRESS, AND ZIP CODE</b> <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>	<b>b. CAGE CODE</b> <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>
<b>c. COGNIZANT SECURITY OFFICE(S) (CSO)</b> <i>(Name, Address, ZIP Code, Telephone required; Email Address optional)</i> <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>	
<b>8. ACTUAL PERFORMANCE</b> <i>(Click button to add more locations)</i>	
<div style="display: flex; justify-content: flex-end; gap: 10px;"> <span>Add Row</span> <span>Remove last Row</span> <span>Delete All Rows</span> </div>	
<b>a. LOCATION(S)</b> <i>(For actual performance, see instructions.)</i> <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>	<b>b. CAGE CODE</b> <i>(If applicable, see instructions.)</i> <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>
<b>c. COGNIZANT SECURITY OFFICE(S) (CSO)</b> <i>(Name, Address, ZIP Code, Telephone required; Email Address optional)</i> <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>	
<b>9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT</b>	

CLASSIFICATION (When filled in): <span style="border: 1px solid black; padding: 2px;">Unclassified</span>							
<b>10. CONTRACTOR WILL REQUIRE ACCESS TO:</b> <i>(X all that apply. Provide details in Blocks 13 or 14 as set forth in the instructions.)</i> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top; padding: 5px;"> <input type="checkbox"/> a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION  <input type="checkbox"/> b. RESTRICTED DATA  <input type="checkbox"/> c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)  <i>(If CNWDI applies, RESTRICTED DATA must also be marked.)</i>  <input type="checkbox"/> d. FORMERLY RESTRICTED DATA  <input checked="" type="checkbox"/> e. NATIONAL INTELLIGENCE INFORMATION:  <div style="margin-left: 20px;"> <input type="checkbox"/> (1) Sensitive Compartmented Information (SCI)  <input type="checkbox"/> (2) Non-SCI </div> </td> <td style="width: 50%; vertical-align: top; padding: 5px;"> <input type="checkbox"/> f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION  <input type="checkbox"/> g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION  <input type="checkbox"/> h. FOREIGN GOVERNMENT INFORMATION  <input type="checkbox"/> i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION  <input type="checkbox"/> j. CONTROLLED UNCLASSIFIED INFORMATION (CUI)  <i>(See instructions.)</i>  <input type="checkbox"/> k. OTHER (Specify) <i>(See instructions.)</i> </td> </tr> </table>		<input type="checkbox"/> a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION <input type="checkbox"/> b. RESTRICTED DATA <input type="checkbox"/> c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) <i>(If CNWDI applies, RESTRICTED DATA must also be marked.)</i> <input type="checkbox"/> d. FORMERLY RESTRICTED DATA <input checked="" type="checkbox"/> e. NATIONAL INTELLIGENCE INFORMATION: <div style="margin-left: 20px;"> <input type="checkbox"/> (1) Sensitive Compartmented Information (SCI)  <input type="checkbox"/> (2) Non-SCI </div>	<input type="checkbox"/> f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION <input type="checkbox"/> g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION <input type="checkbox"/> h. FOREIGN GOVERNMENT INFORMATION <input type="checkbox"/> i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION <input type="checkbox"/> j. CONTROLLED UNCLASSIFIED INFORMATION (CUI) <i>(See instructions.)</i> <input type="checkbox"/> k. OTHER (Specify) <i>(See instructions.)</i>				
<input type="checkbox"/> a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION <input type="checkbox"/> b. RESTRICTED DATA <input type="checkbox"/> c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) <i>(If CNWDI applies, RESTRICTED DATA must also be marked.)</i> <input type="checkbox"/> d. FORMERLY RESTRICTED DATA <input checked="" type="checkbox"/> e. NATIONAL INTELLIGENCE INFORMATION: <div style="margin-left: 20px;"> <input type="checkbox"/> (1) Sensitive Compartmented Information (SCI)  <input type="checkbox"/> (2) Non-SCI </div>	<input type="checkbox"/> f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION <input type="checkbox"/> g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION <input type="checkbox"/> h. FOREIGN GOVERNMENT INFORMATION <input type="checkbox"/> i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION <input type="checkbox"/> j. CONTROLLED UNCLASSIFIED INFORMATION (CUI) <i>(See instructions.)</i> <input type="checkbox"/> k. OTHER (Specify) <i>(See instructions.)</i>						
<b>11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</b> <i>(X all that apply. See instructions. Provide details in Blocks 13 or 14 as set forth in the instructions.)</i> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top; padding: 5px;"> <input type="checkbox"/> a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY  <i>(Applicable only if there is no access or storage required at contractor facility. See instructions.)</i>  <input type="checkbox"/> b. RECEIVE AND STORE CLASSIFIED DOCUMENTS ONLY  <input type="checkbox"/> c. RECEIVE, STORE, AND GENERATE CLASSIFIED INFORMATION OR MATERIAL  <input type="checkbox"/> d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE  <input type="checkbox"/> e. PERFORM SERVICES ONLY  <input type="checkbox"/> f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES </td> <td style="width: 50%; vertical-align: top; padding: 5px;"> <input type="checkbox"/> g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER  <input type="checkbox"/> h. REQUIRE A COMSEC ACCOUNT  <input type="checkbox"/> i. HAVE A TEMPEST REQUIREMENT  <input type="checkbox"/> j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS  <input type="checkbox"/> k. BE AUTHORIZED TO USE DEFENSE COURIER SERVICE  <input type="checkbox"/> l. RECEIVE, STORE, OR GENERATE CONTROLLED UNCLASSIFIED INFORMATION (CUI).  <i>(DoD Components: refer to DoDM 5200.01, Volume 4 only for specific CUI protection requirements. Non-DoD Components: see instructions.)</i>  <input type="checkbox"/> m. OTHER (Specify) <i>(See instructions.)</i> </td> </tr> </table>		<input type="checkbox"/> a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY <i>(Applicable only if there is no access or storage required at contractor facility. See instructions.)</i> <input type="checkbox"/> b. RECEIVE AND STORE CLASSIFIED DOCUMENTS ONLY <input type="checkbox"/> c. RECEIVE, STORE, AND GENERATE CLASSIFIED INFORMATION OR MATERIAL <input type="checkbox"/> d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE <input type="checkbox"/> e. PERFORM SERVICES ONLY <input type="checkbox"/> f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input type="checkbox"/> g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER <input type="checkbox"/> h. REQUIRE A COMSEC ACCOUNT <input type="checkbox"/> i. HAVE A TEMPEST REQUIREMENT <input type="checkbox"/> j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS <input type="checkbox"/> k. BE AUTHORIZED TO USE DEFENSE COURIER SERVICE <input type="checkbox"/> l. RECEIVE, STORE, OR GENERATE CONTROLLED UNCLASSIFIED INFORMATION (CUI). <i>(DoD Components: refer to DoDM 5200.01, Volume 4 only for specific CUI protection requirements. Non-DoD Components: see instructions.)</i> <input type="checkbox"/> m. OTHER (Specify) <i>(See instructions.)</i>				
<input type="checkbox"/> a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY <i>(Applicable only if there is no access or storage required at contractor facility. See instructions.)</i> <input type="checkbox"/> b. RECEIVE AND STORE CLASSIFIED DOCUMENTS ONLY <input type="checkbox"/> c. RECEIVE, STORE, AND GENERATE CLASSIFIED INFORMATION OR MATERIAL <input type="checkbox"/> d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE <input type="checkbox"/> e. PERFORM SERVICES ONLY <input type="checkbox"/> f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input type="checkbox"/> g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER <input type="checkbox"/> h. REQUIRE A COMSEC ACCOUNT <input type="checkbox"/> i. HAVE A TEMPEST REQUIREMENT <input type="checkbox"/> j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS <input type="checkbox"/> k. BE AUTHORIZED TO USE DEFENSE COURIER SERVICE <input type="checkbox"/> l. RECEIVE, STORE, OR GENERATE CONTROLLED UNCLASSIFIED INFORMATION (CUI). <i>(DoD Components: refer to DoDM 5200.01, Volume 4 only for specific CUI protection requirements. Non-DoD Components: see instructions.)</i> <input type="checkbox"/> m. OTHER (Specify) <i>(See instructions.)</i>						
<b>12. PUBLIC RELEASE</b> 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. <i>(See instructions)</i> <table style="width: 100%; border: none;"> <tr> <td style="width: 33%; border: none;"> <input type="checkbox"/> DIRECT </td> <td style="width: 33%; border: none;"> <input type="checkbox"/> THROUGH <i>(Specify below)</i> </td> <td style="width: 34%; border: none;"> <b>Public Release Authority:</b> </td> </tr> <tr> <td colspan="3" style="height: 40px; border: none;"></td> </tr> </table>		<input type="checkbox"/> DIRECT	<input type="checkbox"/> THROUGH <i>(Specify below)</i>	<b>Public Release Authority:</b>			
<input type="checkbox"/> DIRECT	<input type="checkbox"/> THROUGH <i>(Specify below)</i>	<b>Public Release Authority:</b>					
<b>13. SECURITY GUIDANCE</b> <div style="float: right; text-align: right;"> <span style="border: 1px solid black; padding: 2px 5px;">Add Signature</span> <span style="border: 1px solid black; padding: 2px 5px;">Remove last Signature</span> <span style="border: 1px solid black; padding: 2px 5px;">Delete All Signatures</span> </div> <p>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.</p> <p><i>(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.)</i></p> <div style="border: 1px solid black; height: 100px; margin-top: 10px;"></div>							
List of Attachments (All Files Must be Attached Prior to Signing, i.e., for any digital signature on the form) <div style="border: 1px solid black; height: 150px; margin-top: 10px;"></div>							
<div style="display: flex; justify-content: space-between; border-top: 1px solid black;"> <span>Add Attachment</span> <span>View Selected Attachment</span> <span>Remove Selected Attachment</span> </div>							

DD FORM 254, APR 2018

PREVIOUS EDITION IS OBSOLETE.

CLASSIFICATION (When filled in): Unclassified

Page 2 of 3  
AEM Lifecycle Designer

10 Feb 25

CLASSIFICATION (When filled in): <span style="border: 1px solid black; padding: 0 5px;">Unclassified</span>		
NAME & TITLE OF REVIEWING OFFICIAL		SIGNATURE
<b>14. ADDITIONAL SECURITY REQUIREMENTS</b> Requirements, in addition to NISPOM requirements for classified information, are established for this contract. <div style="display: flex; align-items: flex-start;"><div style="margin-right: 10px;"><input type="checkbox"/> No    <input type="checkbox"/> Yes</div><div><small>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.)</small></div></div> <div style="height: 60px; border: 1px solid black; margin-top: 5px;"></div>		
<b>15. INSPECTIONS</b> Elements of this contract are outside the inspection responsibility of the CSO. <div style="display: flex; align-items: flex-start;"><div style="margin-right: 10px;"><input type="checkbox"/> No    <input type="checkbox"/> Yes</div><div><small>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.)</small></div></div> <div style="height: 60px; border: 1px solid black; margin-top: 5px;"></div>		
<b>16. GOVERNMENT CONTRACTING ACTIVITY (GCA) AND POINT OF CONTACT (POC)</b>		
a. GCA NAME	c. ADDRESS (Include ZIP Code)	d. POC NAME
b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE (See Instructions)		e. POC TELEPHONE (Include Area Code)
		f. EMAIL ADDRESS (See Instructions)
<b>17. CERTIFICATION AND SIGNATURES</b> 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)	d. AAC OF THE CONTRACTING OFFICE (See Instructions)	h. SIGNATURE
b. TITLE	e. CAGE CODE OF THE PRIME CONTRACTOR (See Instructions.)	
c. ADDRESS (Include ZIP Code)	f. TELEPHONE (Include Area Code)	i. DATE SIGNED (See Instructions)
	g. EMAIL ADDRESS (See Instructions)	
<b>18. REQUIRED DISTRIBUTION BY THE CERTIFYING OFFICIAL</b> <div style="display: flex; justify-content: space-between;"><div style="width: 45%;"><div style="margin-bottom: 5px;"><input type="checkbox"/> a. CONTRACTOR</div><div style="margin-bottom: 5px;"><input type="checkbox"/> b. SUBCONTRACTOR</div><div style="margin-bottom: 5px;"><input type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR</div><div style="margin-bottom: 5px;"><input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION</div><div style="margin-bottom: 5px;"><input type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER</div></div><div style="width: 50%;"><div style="margin-bottom: 5px;"><input type="checkbox"/> f. OTHER AS NECESSARY (If more room is needed, continue in Item 13 or on additional page if necessary.)</div><div style="height: 80px; border: 1px solid black; margin-top: 5px;"></div></div></div>		

DD FORM 254, APR 2018

PREVIOUS EDITION IS OBSOLETE.

CLASSIFICATION (When filled in): Unclassified

Page 3 of 3  
AEM LiveCycle Designer



10 Feb 25

## DD FORM 254, SCI ADDENDUM TEMPLATE

RELEASE OF SENSITIVE COMPARTMENTED INFORMATION (SCI)  
INTELLIGENCE INFORMATION TO U.S. CONTRACTORS

ATTACHMENT TO DD FORM 254 FOR SOLICITATION/CONTRACT NO.: #####

ORDER NO.: #####

SUBCONTRACT NO.: #####

CONTRACT ESTIMATED COMPLETION DATE (ECD): #####

SCI NETWORK ACCESS REQUIRED: please list (e.g., JWICS)

The Cognizant Senior Intelligence Officer (SIO) has exclusive security responsibility for all Sensitive Compartmented Information (SCI) classified material released to or developed under the contract. Access to SCI Intelligence material requires adherence to the requirements set forth in the following: Department of Defense (DoD) Manual (DoDM) 5105.21, Volume 1, SCI Administrative Security Manual: Administration of Information and Information Systems Security; DoDM 5105.21, Volume 2, SCI Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security; DoDM 5105.21, Volume 3, SCI Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities; ICD 403, Foreign Disclosure and Release of Classified National Intelligence; ICD 701, Security Policy Directive for Unauthorized Disclosures of Classified Information; ICD 703 Protection of Classified National Intelligence Including Sensitive Compartmented Information; ICS 703-02, Reporting Requirements for Individuals with Access to Sensitive Compartmented Information; ICS 703-03, Protection of Classified National Intelligence Including SCI Shared with Entities Outside the Intelligence Community; ICS 703-04, Foreign Ownership, Control, or Influence (FOCI); ICD 710, Classification Management and Control Markings Systems; ICPG 710.1, Application of Dissemination Controls: Originator Control (ORCON); DoD 5220.22-M, Change 2, National Industrial Security Program Operating Manual (NISPOM); DoDM 5200.01, Volumes 1-3, DoD Information Security Program; DoDI 5200.48, Controlled Unclassified Information (CUI); and Security Executive Agent Directive (SEAD) 3, Reporting Requirements for Personnel with Access to Classified Information or who hold a Sensitive Position. Contractor's will comply with all regulations/manuals/directives stated therein which provide the necessary security and classification guidance for personnel, information, physical, automated information security (AIS), and technical security measures and is a part of the SCI security specifications for the contract. Inquiries pertaining to SCI classification guidance or interpretations shall be directed to the Contracting Officer/Contracting Officer Representative (COR) identified on the attached DD Form 254.

## 1. Requirements for access to SCI:

- a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated Special Security Officer (SSO).
- b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated COR.
- c. 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 COR.

10 Feb 25

**RELEASE OF SENSITIVE COMPARTMENTED INFORMATION (SCI)  
INTELLIGENCE INFORMATION TO U.S. CONTRACTORS**

**ATTACHMENT TO DD FORM 254 FOR SOLICITATION/CONTRACT NO.: #####****ORDER NO.: #####****SUBCONTRACT NO.: #####****CONTRACT ESTIMATED COMPLETION DATE (ECD): #####****SCI NETWORK ACCESS REQUIRED: please list (e.g., JWICS)**

- d. Names of contractor personnel requiring access to SCI will be submitted to the COR for approval. (The COR is identified on the DD Form 254.) Upon receipt of written approval from the COR, the company security officer will submit request(s) for special background investigations, in accordance with the NISPOM, to the Defense Security Service (DSS).
- e. SCI material must not be released to foreign nationals or immigrant aliens whether they are consultants, U.S. 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 COR and shall include:
  - i. A copy of the proposed disclosure.
  - ii. Full justification reflecting the benefits to U.S. interests.
  - iii. Name, nationality, particulars of clearance, and current access authorization of each proposed foreign national recipient.
- f. Contractor personnel must maintain accountability for all intelligence materials released to their custody.
- g. SCI material will not be reproduced without prior approval of the originator of the material. All SCI material shall bear a prohibition against reproduction while in the contractor's custody.
- h. Inquiries pertaining to classification guidance on SCI will be directed through the CSSO to the responsible COR as indicated on the DD Form 254.
- i. SCI released to cleared-DoD Contractors, all reproductions thereof, and all other information generated based on, or incorporating data from, in support of this contract, remains the property of the U.S. Government. Upon completion or cancellation of the contract, all SCI material furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the COR.
- j. SCI will be stored and maintained only in properly accredited facilities meeting the physical security requirements in ICD 705, SCI Facilities and ICS 705, Technical Specifications for Construction and Management of SCI Facilities.
- k. The **add Command Name** SSO will recognize the above noted estimated completion date (ECD) as the completion date for the contract. The SSO will initiate action to debrief

10 Feb 25

RELEASE OF SENSITIVE COMPARTMENTED INFORMATION (SCI)  
INTELLIGENCE INFORMATION TO U.S. CONTRACTORS

ATTACHMENT TO DD FORM 254 FOR SOLICITATION/CONTRACT NO.: #####

ORDER NO.: #####

SUBCONTRACT NO.: #####

CONTRACT ESTIMATED COMPLETION DATE (ECD): #####

SCI NETWORK ACCESS REQUIRED: *please list (e.g., JWICS)*

contractor personnel with access to this contract unless extensions or modifications to the contract are received by the SSO office no later than 30 days after the established completion date.

1. The contractor is governed by ICD 704, *'Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI) And Other Controlled Access Program Information'* and may be supplemented by SSO Navy guidance. Contractor personnel, assigned to this contract, that are eligible for access to SCI or currently possess an SCI personnel security clearance with another non-DoD agency must have their SCI eligibility adjudicated by the DoD Consolidated Adjudications Facility (CAF) prior to having access to SCI information retained by add Command Name, unescorted access to add Command Name spaces, and receipt of an add Command Name issued contractor badge. The contractor will identify, in writing, contractor personnel assigned to this contract by NAME, SSN, Date and Place of Birth, and provide this documentation to the CO/COR identified on the DD 254. The CO/COR will identify the SCI caveats for the contract and forward a copy of this documentation to the SSO for processing. This documentation will be marked and protected under the Privacy Act of 1974.
- m. Electronic processing of SCI must be accomplished on equipment accredited in accordance with DoDM 5105.21 Volumes 1- 3, ICD 503, Information Technology System Security Risk Management, Certification and Accreditation, and the DoDIIS Joint Security Implementation Guide (DJSIG), Appendix D.
- n. SCI security management issues shall be directed to add Command SSO and telephone number
- o. In accordance with Director of National Intelligence Memorandum 5 May 2017, Access to North Atlantic Treaty Organization (NATO) Information by Intelligence Community (IC) Personnel and Naval Intelligence Security Policy Directive 17-008 Revision, Mandate for North Atlantic Treaty Organization (NATO) Information by Intelligence Community (IC) Personnel, all DoN Contractors with SCI access and access to JWICS or SIPRNet must be briefed into NATO Secret Information.

**\*\*NOTE\*\*:** ADDITIONAL SECURITY GUIDANCE SPECIFIC TO THE SCI CONTRACT WILL BE PROVIDED BY THE COR AND COMMAND SSO TO IDENTIFY SECURITY CLASSIFICATION GUIDES AND PROGRAM SPECIFIC SECURITY GUIDANCE THAT DEFINE TECHNICAL AND SAFEGUARDING REQUIREMENTS IDENTIFIED IN THE SOW/PWS/SOO.

## COMPLETE PACKAGE CHECKLIST

1. Complete packages will include the following:
  - a. A complete and accurate SOW or PWS.
  - b. Encl (3).
  - c. Encl (4)
  - d. Encl (10) and Encl (11) if required.
  - e. Encl (6) with the following endorsements by Commander (COMNAVRESFOR or COMNAVRESFORCOM), as applicable:
    - (1) Request for SAIRC support.
    - (2) One or more SAIRC criteria clearly identified.
    - (3) Proposed contracting action falls within the scope-of-authority of the Sponsoring Command.
    - (4) Risk Assessment that focuses on potential risks to Department of the Navy (DON) equities and DON's acceptance of risk.
    - (5) Proposed contract action is executable by allocation of specialized, limited-availability DON resources.