

FOIA Electronic Reading Room Document Coversheet

Document Description: N68936-01-D-0037 Contract Mods P00001 - P00003

This document has been released in its entirety.

Portions of this document have been excised pursuant to the Freedom of Information Act. The applicable portion(s) excised and the exemption(s) applied are below indicated.

- Exemption (b)(1) Information excised is properly and currently classified in the interest of national defense or foreign policy
- Exemption (b)(2) Information excised is related solely to the internal rules and practices of the Agency.
- Exemption (b)(3) Information excised is specifically exempt from disclosure by an Executive Order or Statute. Specifically:
- Exemption (b)(4) Information excised is commercial or financial information received from outside the Government and is likely to cause substantial harm to the competitive position of the source providing the information.
- Exemption (b)(5) Information excised is internal advice, recommendations, or subjective evaluations pertaining to the decision-making process of the Agency.
- Exemption (b)(6) Information excised is certain individual names and personal identifiers and is excised for heightened interest in the personal privacy of Department of Defense personnel that is concurrent with the increased security awareness demands.
- Exemption (b) (7) Information excised is investigatory records or information compiled for law enforcement purposes
- Exemption (b)(8) Information excised is records for the use of any agency responsible for the regulation or supervision of financial institutions
- Exemption (b)(9) Information excised is records containing geological and geophysical information (including maps) concerning wells.

Please direct inquiries regarding this document to:
Commander (Code K00000D FOIA)
Naval Air Warfare Center Weapons Division
1 Administration Circle Stop 1009
China Lake, CA 93555-6100.

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT				1. CONTRACT ID CODE	PAGE OF PAGES
2. AMENDMENT/MODIFICATION NO. P00001		3. EFFECTIVE DATE 13-Sep-2001	4. REQUISITION/PURCHASE REQ. NO. N60530-0290-CYBC	5. PROJECT NO.(If applicable)	
6. ISSUED BY CDR NAWCWD CODE 210000D ATTN: S. LAMBERT (760) 939-7652 1 ADMIN CIR, BLDG 982 CHINA LAKE CA 93555-6100		CODE N68936	7. ADMINISTERED BY (If other than item 6) DCM BALTIMORE 217 E. REDWOOD, SUITE 1800 BALTIMORE MD 21202-5299		CODE S2101A
8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and Zip Code) THE SURVICE ENGINEERING COMPANY JAMES B. FOULK SURVICE ENGINEERING COMPANY 1003 OLD PHILADELPHIA ROAD SUITE 103 ABERDEEN MD 21001-4011				9A. AMENDMENT OF SOLICITATION NO.	
				9B. DATED (SEE ITEM 11)	
CODE 7T988				FACILITY CODE	
				X 10A. MOD. OF CONTRACT/ORDER NO. N68936-01-D-0037	
				X 10B. DATED (SEE ITEM 13) 26-Jul-2001	
11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS					
<input type="checkbox"/> The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offer <input type="checkbox"/> is extended, <input type="checkbox"/> is not extended.					
Offer must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.					
12. ACCOUNTING AND APPROPRIATION DATA (If required)					
13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.					
A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.					
B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(B).					
C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:					
X D. OTHER (Specify type of modification and authority) Mutual agreement of both parties.					
E. IMPORTANT: Contractor <input type="checkbox"/> is not, <input checked="" type="checkbox"/> is required to sign this document and return _____ copies to the issuing office.					
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.) See pages herein					
Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.					
15A. NAME AND TITLE OF SIGNER (Type or print)			16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) DIANE E FOUCHER / PROCUREMENT CONTRACTING OFFICE		
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA		16C. DATE SIGNED	
(Signature of person authorized to sign)		BY <u>Diane E. Foucher</u>		13-Sep-2001	
		(Signature of Contracting Officer)			

EXCEPTION TO SF 30
APPROVED BY OIRM 11-84

30-105-04

STANDARD FORM 30 (Rev. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

Changes in Section F

The following clauses which are incorporated by full text have been added or modified:

F-TXT PLACE OF PERFORMANCE

- (a) All task orders shall be performed at the Naval Air Warfare Center, Weapons Division, China Lake, CA or at the contractor's facility in or near Ridgecrest, CA, unless another location is specified in the task order. Accordingly, the contractor shall maintain within a 30 mile radius of the NAWCWD, China Lake, main gate, an office with the capability to provide services and resources to accomplish the work described in this Statement of Work. The contractor shall provide management and administrative support for the office sufficient to provide work direction, planning, and progress and schedule status reporting for the task order contract. All efforts will be initiated by Task Orders which will specify completely the requirements and deliverables.
- (b) The contractor shall supply all equipment, facilities, space and materials necessary for the technical, management and administration of the work performed under this contract at the contractor's facility.
- (c) The government will provide access to equipment, facilities, space and materials for work performed at the Naval Air Warfare Center, Weapons Division, China Lake, CA

Changes in Section G

Summary for the Payment Office

The total funded amount of the contract remains unchanged.

The following clauses which are incorporated by full text have been added or modified:

G-TXT-06 SECURITY ASSIGNMENT

Defense Security Service Capitol Region, 938 Elkridge Landing Road, Linthicum, MD 21090 is hereby assigned administrative responsibility for safeguarding classified information.

G-TXT-07 PAYMENT ADDRESS

Payment under this contract shall be sent to the following address:

SURVICE Engineering Company
4695 Millennium Dr.
Belcamp, MD 21017

G-TXT-13 COURTESY COPY OF INVOICE/VOUCHER

A courtesy copy of each invoice/voucher processed for payment will be sent to:

COMMANDER
CODE 761500D
NAVAIRWARCENWPNDIV
1 ADMINISTRATION CIRCLE
CHINA LAKE CA 93555-6100

CONTRACTING OFFICE:

COMMANDER
CODE 210000D (S. Lambert - 760-939-7652)
NAVAIRWARCENWPNDIV
1 ADMINISTRATIVE CIRCLE
CHINA LAKE, CA 93555-6100

COR:

COMMANDER

CODE 218100D (J. Tucker – 760-939-8442)
NAVAIRWARCENWPNDIV
1 ADMINISTRATIVE CIRCLE
CHINA LAKE, CA 93555-6100
Changes in Section H

The following clauses which are incorporated by full text have been added or modified:

5252.209-9510 ORGANIZATIONAL CONFLICTS OF INTEREST (SERVICES) (JUL 1998)

(a) Purpose. This clause seeks to ensure that the contractor (1) does not obtain an unfair competitive advantage over other parties by virtue of its performance of this contract, and (2) is not biased because of its current or planned interests (financial, contractual, organizational or otherwise) that relate to the work under this contract.

(b) Scope. The restrictions described herein shall apply to performance or participation by the contractor (as defined in paragraph (d)(7)) in the activities covered by this clause.

(1) The restrictions set forth in paragraph (e) apply to supplies, services, and other performance rendered with respect to the suppliers and/or equipment listed in the Statement of Work contained in Section C. Delivery orders/Task orders issued under the contract will specify to which suppliers and/or equipment subparagraph (e) restrictions apply.

(2) The financial, contractual, organizational and other interests of contractor personnel performing work under this contract shall be deemed to be the interests of the contractor for the purposes of determining the existence of an Organizational Conflict of Interest. Any subcontractor that performs any work relative to this contract shall be subject to this clause. The contractor agrees to place in each subcontract affected by these provisions the necessary language contained in this clause.

(c) Waiver. Any request for waiver of the provisions of this clause shall be submitted in writing to the Procuring Contracting Officer. The request for waiver shall set forth all relevant factors including proposed contractual safeguards or job procedures to mitigate conflicting roles that might produce an Organizational Conflict of Interest. No waiver shall be granted by the Government with respect to prohibitions pursuant to access to proprietary data.

(d) Definitions. For purposes of application of this clause only, the following definitions are applicable:

(1) "System" includes system, major component, subassembly or subsystem, project, or item.

(2) "Nondevelopmental items" are as defined in FAR 2.101.

(3) "Systems Engineering" (SE) includes, but is not limited to, the activities in FAR 9.505-1(b).

(4) "Technical direction" (TD) includes, but is not limited to, the activities in FAR 9.505-1(b).

(5) "Advisory and Assistance Services" (AAS) are those services acquired from non-governmental sources to support or improve agency policy development or decision making; or, to support or improve the management of organizations or the operation of hardware systems. Such services may encompass consulting activities, engineering and technical services, management support services and studies, analyses and evaluations.

(6) "Consultant" services is as defined in FAR 31.205-33(a).

(7) "Contractor", for the purposes of this clause, means the firm signing this contract, its subsidiaries and affiliates, joint ventures involving the firm, any entity with which the firm may hereafter merge or affiliate, and any other successor or assignee of the firm.

(8) "Affiliates" means officers or employees of the prime contractor and first tier subcontractors involved in the program and technical decision making process concerning this contract.

(9) "Interest" means organizational or financial interest.

(10) "Weapons system supplier" means any prime contractor or first tier subcontractor engaged in, or having a known prospective interest in the development, production or analysis of any of the weapon systems, as well as any major component or subassembly of such system.

(e) Contracting restrictions.

(1) To the extent the contractor provides systems engineering and/or technical direction for a system or commodity but does not have overall contractual responsibility for the development, the integration, assembly and checkout (IAC) or the production of the system, the contractor shall not (i) be awarded a contract to supply the system or any of its major components or (ii) be a subcontractor or consultant to a supplier of the system or of its major components. The contractor agrees that it will not supply to the Department of Defense (either as a prime contractor or as a subcontractor) or act as consultant to a supplier of, any system, subsystem, or major component utilized for or in connection with any item or other matter that is (directly or indirectly) the subject of the systems

engineering and/or technical direction or other services performed under this contract for a period of three (3) years after the date of completion of the contract. (FAR 9.505-1(a))

(2) To the extent the contractor prepares and furnishes complete specifications covering nondevelopmental items to be used in a competitive acquisition, the contractor shall not be allowed to furnish these items either as a prime contractor or subcontractor. This rule applies to the initial production contract, for such items plus a specified time period or event. The contractor agrees to prepare complete specifications covering non-developmental items to be used in competitive acquisitions, and the contractor agrees not to be a supplier to the Department of Defense, subcontract supplier, or a consultant to a supplier of any system or subsystem for which complete specifications were prepared hereunder. The prohibition relative to being a supplier, a subcontract supplier, or a consultant to a supplier of these systems of their subsystems extends for a period of two (2) years after the terms of this contract. (FAR 9.505-2(a)(1))

(3) To the extent the contractor prepares or assists in preparing a statement of work to be used in competitively acquiring a system or services or provides material leading directly, predictably and without delay to such a work statement, the contractor may not supply the system, major components thereof or the services unless the contractor is the sole source, or a participant in the design or development work, or a contractor involved in preparation of the work statement. The contractor agrees to prepare, support the preparation of or provide material leading directly, predictably and without delay to a work statement to be used in competitive acquisitions, and the contractor agrees not to be a supplier or consultant to a supplier of any services, systems or subsystems for which the contractor participated in preparing the work statement. The prohibition relative to being a supplier, a subcontract supplier, or a consultant to a supplier of any services, systems or subsystems extends for a period 2 years after the terms of this contract. (FAR 9.505-2(a)(1))

(4) To the extent work to be performed under this contract requires evaluation of offers for products or services, a contract will not be awarded to a contractor that will evaluate its own offers for products or services, or those of a competitor, without proper safeguards to ensure objectivity to protect the Government's interests. Contractor agrees to the terms and conditions set forth in the Statement of Work that are established to ensure objectivity to protect the Government's interests.(FAR 9.505-3)

(5) To the extent work to be performed under this contract requires access to proprietary data of other companies, the contractor must enter into agreements with such other companies which set forth procedures deemed adequate by those companies (i) to protect such data from unauthorized use or disclosure so long as it remains proprietary and (ii) to refrain from using the information for any other purpose other than that for which it was furnished. Evidence of such agreement(s) must be made available to the Procuring Contracting Officer upon request. The contractor shall restrict access to proprietary information to the minimum number of employees necessary for performance of this contract. Further, the contractor agrees that it will not utilize proprietary data obtained from such other companies in preparing proposals (solicited or unsolicited) to perform additional services or studies for the United States Government. The contractor agrees to execute agreements with companies furnishing proprietary data in connection with work performed under this contract, obligating the contractor to protect such data from unauthorized use or disclosure so long as such data remains proprietary, and to furnish copies of such agreement to the Contracting Officer. Contractor further agrees that such proprietary data shall not be used in performing for the Department of Defense additional work in the same field as work performed under this contract if such additional work is procured competitively. (FAR 9.505-4(b))

(6) Preparation of Statements of Work or Specifications. If the contractor under this contract assists substantially in the preparation of a statement of work or specifications, the contractor shall be ineligible to perform or participate in any capacity in any contractual effort (solicited or unsolicited) which is based on such statement of work or specifications. The contractor shall not incorporate its products or services in such statement of work or specifications unless so directed in writing by the Contracting Officer, in which case the restrictions in this subparagraph shall not apply. Contractor agrees that it will not supply to the Department of Defense (either as a prime contractor or as a subcontractor) or act as consultant to a supplier of, any system, subsystem or major component utilized for or in connection with any item or work statement prepared or other services performed or materials delivered under this contract, and is procured on a competitive basis, by the Department of Defense with 2 years after completion of work under this contract. The provisions of this clause shall not apply to any system, subsystem, or major component for which the contractor is the sole source of supply or which it participated in designing or developing. (FAR 9.505-4(b))

(7) Advisory and Assistance Services (AAS). If the contractor provides AAS services as defined in paragraph (d) of this clause, it shall be ineligible thereafter to participate in any capacity in Government contractual efforts (solicited or unsolicited) which stem directly from such work, and the contractor agrees not to perform similar work

for prospective offerors with respect to any such contractual efforts. Furthermore, unless so directed in writing by the Contracting Officer, the contractor shall not perform any such work under this contract on any of its products or services, or the products or services of another firm or which the contractor performs similar work. Nothing in this subparagraph shall preclude the contractor from competing for follow-on contracts for AAS.

(f) Remedies. In the event the contractor fails to comply with the provisions of this clause, such noncompliance shall be deemed a material breach of the provisions of this contract. If such noncompliance is the result of conflicting financial interest involving contractor personnel performing work under this contract, the Government may require the contractor to remove such personnel from performance of work under this contract. Further, the Government may elect to exercise its right to terminate for default in the event of such noncompliance. Nothing herein shall prevent the Government from electing any other appropriate remedies afforded by other provisions of this contract, or statute or regulation.

(g) Disclosure of Potential Conflicts of Interest. The contractor recognizes that during the term of this contract, conditions may change which may give rise to the appearance of a new conflict of interest. In such an event, the contractor shall disclose to the Government information concerning the new conflict of interest. The contractor shall provide, as a minimum, the following information:

- (1) a description of the new conflict of interest (e.g., additional weapons systems supplier(s), corporate restructuring, new first-tier subcontractor(s), new contract) and identity of parties involved;
- (2) a description of the work to be performed;
- (3) the dollar amount;
- (4) the period of performance; and
- (5) a description of the contractor's internal controls and planned actions, to avoid any potential organizational conflict of interest.

Changes in Section J

The free form item "Table of Contents" has been deleted.

The following clauses which are incorporated by full text have been added or modified:

J-TXT-01 SECTION J - LIST OF ATTACHMENTS

TITLE	DATE	NO. OF PAGES
Exhibit A – DD FORM 1423, Contracts Data Requirements List	08/29/01	7
Attachment 1 – DD FORM 254, Contract Security Classification Specification	08/23/01	25

DATA ITEM DESCRIPTIONForm Approved
OMB No 0704-0188

1. TITLE

Performance and Cost Report

2. IDENTIFICATION NUMBER

DI-FNCL-80912

3. DESCRIPTION/PURPOSE

3.1 The Performance and Cost Report provides current status and projected requirements of funds, man-hours, and work completion.

3.2 The report is used for evaluation of contractor progress.

4. APPROVAL DATE
(YYMMDD)

891006

5. OFFICE (IF PRIMARY RESPONSIBILITY (OPR))

A/MICOM

6a. DTIC APPLICABLE

6b. GDSF APPLICABLE

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated by the specific and discrete task requirement as delineated in the contract.

7.2 This DID supersedes DI-F-1288A.

8. APPROVAL LIMITATION

9a. APPLICABLE FORMS

9b. AMSC NUMBER

A4845

10. PREPARATION INSTRUCTIONS

10.1 Format. The Performance and Cost Report format shall be contractor selected. Unless effective presentation would be degraded, the initially used format arrangement shall be used for all subsequent submissions.

10.2 Content. The Performance and Cost Report shall contain the following:

10.2.1 Man-hours. Total man-hours expended by technical categories or program tasks, cumulative total man-hours to date, and percentages of total man-hours spent to date. State whether or not remaining hours are sufficient to complete the task.

10.2.2 Funds. Total funds expended, by task, for the month; cumulative total funds spent to date; and percentage of total contract funds spent to date. State whether or not remaining funds are sufficient to complete the task.

10.2.3 Work completion. Percentage of work completed, by tasks during the month, and cumulative percentage of total contract work completed to date.

11. DISTRIBUTION STATEMENT

DISTRIBUTION STATEMENT A:

Approved for public release; distribution is unlimited.

DATA ITEM DESCRIPTION

Form Approved
GSA No. 0704-0188
Exp. Date: Jun 30, 1986

1. TITLE Contractor's Progress, Status and Management Report		2. IDENTIFICATION NUMBER DI-MGMT-80227	
3. DESCRIPTION/PURPOSE 3.1 The Contractor's Progress, Status and Management Report indicates the progress of work and the status of the program and of the assigned tasks, reports costs, and informs of existing or potential problem areas.			
4. APPROVAL DATE (YYMMDD) 860905	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) N/SPANAR	6a. DTIC REQUIRED	6b. GDSR REQUIRED
7. APPLICATION/INTERRELATIONSHIP 7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated by the specific and discrete task requirement for this data included in the contract. 7.2 This DID may be applied in any contract and during any program phase. 7.3 This DID supersedes DI-A-2090A, DI-A-3025A, UDI-A-22050B, UDI-A-22052A, UDI-A-23960, DI-A-30024, and DI-A-30606. (cont. on page 2)			
8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER N3947	
10. PREPARATION INSTRUCTIONS 10.1 <u>Contract</u> - This data item is generated by the contract which contains a specific and discrete work task to develop this data product. 10.2 <u>Format</u> - This report shall be typewritten on standard size (e.g. 8 1/2" by 11") white paper, and securely stapled. Pages shall be sequentially numbered. All attachments shall be identified and referenced in the text of the report. The report shall be prepared in the contractor's format and shall be legible and suitable for reproduction. 10.3 <u>Content</u> - The report shall include: a. A front cover sheet which includes the contractor's name and address, the contract number, the nomenclature of the system or program, the date of the report, the period covered by the report, the title of the report, either the serial number of the report or the Contract Data Requirements List (CDRL) sequence number, the security classification, and the name of the issuing Government activity; b. Description of the progress made against milestones during the reporting period; c. Results, positive or negative, obtained related to previously-identified problem areas, with conclusions and recommendations; d. Any significant changes to the contractor's organization or method of operation, to the project management network, or to the milestone chart; e. Problem areas affecting technical or scheduling elements, with background and any recommendations for solutions beyond the scope of the contract; f. Problem areas affecting cost elements, with background and any recommendations for solutions beyond the scope of the contract; g. Cost curves showing actual and projected conditions throughout the contract; h. Any cost incurred for the reporting period and total contractual expenditures as of reporting date; i. Person-hours expended for the reporting period and cumulatively for the contract; j. Any trips and significant results; (cont. on page 2)			

7. APPLICATION/INTERRELATIONSHIP (Cont'd)

- 7.4 Paragraphs 10.3.f, 10.3.g, and 10.3.h herein should be tailored on DD Form 1423 when such cost data is already submitted through a sophisticated cost reporting system under the contract.
-

10. PREPARATION INSTRUCTIONS (Cont'd)

- k. Record of all significant telephone calls and any commitments made by telephone;
- l. Summary of Engineering Change Proposal (ECP) status, including identification of proposed ECPs, approved ECPs, and implemented ECPs;
- m. Contract schedule status;
- n. Plans for activities during the following reporting period;
- o. Name and telephone number of preparer of the report;
- p. Appendixes for any necessary tables, references, photographs, illustrations, and charts.

DATA ITEM DESCRIPTION

Title: TECHNICAL REPORT - STUDY/SERVICES

Number: DI-MISC-80508A

Approval Date: 7 November 2000

Office of Primary Responsibility: G/TS-ALS

GIDEP Applicable: No

Applicable Forms: No

AMSC Number: G7408

DTIC Applicable: Defense Technical Information Center (DTIC), 8725 John J. Kingman Rd.,
Ste. 0944, Ft. Belvoir, VA 22060-6218

Use/Relationship

A technical report provides fully documented results of studies or analyses performed. This data item description contains the format and content instructions for the data product generated by the specific and discrete task requirement as delineated in the contract.

This DID supersedes DI-MISC-80508.

Requirements:

1. Format.

- (a) The report and all attachments shall be typewritten, or otherwise clearly lettered, and shall be duplicated using non-fading ink.
- (b) Text shall be prepared on standard letter size paper (8 1/2" x 11").
- (c) When attachments are included, they shall be fully identified, referenced in the text, and folded to conform to the size paper used in the report.
- (d) Security classification and distribution markings shall conform to the requirements of the contract, purchase description and security requirements checklist, as applicable.

2. Content.

- (a) Title Page - Identifies the report by providing contract number, project name or purchase description title, task number, and reporting period.
- (b) Table of Contents
- (c) Section I - Includes the following:
 - (1) Introduction
 - (2) Summary - A brief statement of results obtained from the analytic effort.
 - (3) Conclusions and their condensed technical substantiation's.
- (d) Section II - A complete and detailed description of the analytic results which led to the conclusions stated in Section I above.

**DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION**

*(The requirements of the DoD Industrial Security Manual apply
to all security aspects of this effort)*

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED

TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED

SECRET

Ref# CL00-037

Stub # N605300290CYBC

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

<input checked="" type="checkbox"/>	a. PRIME CONTRACT NUMBER	N68936-01-D-0037	08/07/31
<input type="checkbox"/>	b. SUBCONTRACT NUMBER		
<input type="checkbox"/>	c. SOLICITATION OR OTHER NUMBER	N68936-01-R-0017	Date (Y/M/DCD)

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

<input checked="" type="checkbox"/>	a. ORIGINAL (Complete date in all cases.)	Date (Y/M/DCD)	01/07/11
<input checked="" type="checkbox"/>	b. REVISED (Supersedees all previous specs.)	Revision No. 1	Date (Y/M/DCD)
<input type="checkbox"/>	c. FINAL (Complete item 5 in all cases.)	Date (Y/M/DCD)	01/08/23

4. IS THIS A FOLLOW-ON CONTRACT?

Classified material received or generated under YES NO. If yes, complete the following:
(Preceding Contract Number) is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254?

In response to contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.

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

a. NAME, ADDRESS, AND ZIP CODE THE SURVICE ENGINEERING COMPANY 1003 OLD PHILADELPHIA ROAD SUITE 103 ABERDEEN, MD 21001	b. CAGE CODE 7T988	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE CAPITAL REGION 938 ELKRIDGE LANDING ROAD LINTHICUM, MD 21090
--	------------------------------	--

7. SUBCONTRACTOR

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

8. ACTUAL PERFORMANCE

a. LOCATION SURVICE ENGINEERING COMPANY 301 NORTH HERITAGE DRIVE SUITE 204 RIDGECREST, CA 93555	b. CAGE CODE 1SSD7	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE 41307 12TH STREET WEST, SUITE 5 PALMDALE, CA 93551
---	------------------------------	--

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

PROVIDE AIR WEAPONS SYSTEMS SURVIVABILITY AND SYSTEMS LEVEL ANALYSIS SERVICES. ELEMENTS OF CONTRACT SUPPORT INCLUDE: (1) AIR WEAPON SURVIVABILITY AND LETHALITY ANALYSES; (2) SURVIVABILITY SIMULATION; SYSTEMS ANALYSES; SURVIVABILITY SYSTEMS ENGINEERING ANALYSIS; DEVELOPMENT AND SUPPORT; AND (3) THE DOCUMENTATION INHERENT IN THE ENGINEERING OR ANALYSIS PROCESS.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:

	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>
b. RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION:		
(1) Sensitive Compartmented Information (SCI)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(2) Non-SCI	<input checked="" type="checkbox"/>	<input type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>
g. NATO INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>
k. OTHER (Specify)	<input type="checkbox"/>	<input type="checkbox"/>

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:

	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input checked="" type="checkbox"/>	<input type="checkbox"/>
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input type="checkbox"/>	<input checked="" type="checkbox"/>
e. PERFORM SERVICES ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input type="checkbox"/>	<input checked="" type="checkbox"/>
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>
h. REQUIRE A COMSEC ACCOUNT	<input checked="" type="checkbox"/>	<input type="checkbox"/>
i. HAVE TEMPEST REQUIREMENTS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
k. BE AUTHORIZED TO USE DEFENSE COURIER SERVICE	<input type="checkbox"/>	<input checked="" type="checkbox"/>
l. OTHER (Specify)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
COMSEC ACCOUNT IS FOR STU-111's ONLY.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to the contract shall not be released for public dissemination except as approved by the Information Security Manual or

Direct Through (specify):

COMMANDER, NAVAL AIR WARFARE CENTER, WEAPONS DIV (741100D), CHINA LAKE, CA 93555

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) * for review.
*In the case of non-ODD User Agencies, request for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in the guidance, the contractor is authorized, encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under the 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

FOREIGN AND FOREIGN OWNED, CONTROLLED OR INFLUENCED (FOCI) CONTRACTORS CANNOT BE PERMITTED ACCESS TO THE INFORMATION REQUIRED FOR PRIME CONTRACTOR FULL PERFORMANCE IN THIS CONTRACT. FOREIGN CONTRACTORS INTERESTED IN PARTICIPATING IN THIS CONTRACT IN A SUBCONTRACT CAPABILITY WILL HAVE TO JOIN WITH A U.S. PRIME CONTRACTOR WHO IS SUBJECT TO THE U.S. DEPARTMENT OF STATE EXPORT LICENSING REQUIREMENTS.

CLASSIFIED WORK CANNOT BE PERFORMED UNTIL A FACILITY CLEARANCE HAS BEEN OBTAINED AT THE CLASSIFICATION LEVEL REQUIRED IN BLOCKS "1A" AND "1B".

ACCESS TO INFORMATION UNDER THIS CONTRACT WILL BE KEPT TO A MINIMUM TO MEET OPERATIONAL REQUIREMENTS.

ACCESS TO AND SAFEGUARDING OF COMSEC INFORMATION/MATERIAL WILL BE IN ACCORDANCE WITH DOD 5220.22-M, NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPO) AND DOD 5220.22-S, NISPO, COMSEC SUPPLEMENT OF LATEST ISSUE AND ALL SUBSEQUENT CHANGES..

THE INSTALLATION OF COMSEC EQUIPMENT UNDER THE CONFIGURATION CONTROL OF NSA WILL BE IN ACCORDANCE WITH OPNAVINST 2221.3C, 5510.93, NTISSI 4000, AND NACSI 4009.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements in addition to ISM requirements, are established for this contract. (If Yes, identify pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of such requirements to the cognizant security office. Use Item 13 if additional space is needed).

Yes No

ADDITIONAL SECURITY REQUIREMENTS HAVE BEEN ADDED TO ITEM 13.

15. Inspections. Elements of the contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the entity responsible for inspections. Use Item 13 if additional space is needed).

Yes No

SPECIFIC ELEMENTS HAVE BEEN ADDED TO ITEM 13.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL
JUDITH K. SMITH

b. TITLE
CONTRACTING OFFICER FOR
SECURITY MATTERS

c. TELEPHONE (include Area Code)
(805) 989-7859

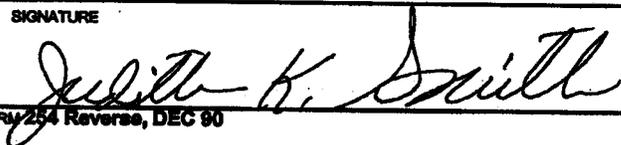
d. ADDRESS (include Zip Code)
COMMANDER
CODE 741100D
NAVAIRWARCENWPNDIV
1 ADMINISTRATION CIRCLE
CHINA LAKE, CA 93555-8001

17. REQUIRED DISTRIBUTION

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

741100E, 210000D, 418100D, 7G0000D

e. SIGNATURE



Prir

USE OF STU-III FOR TRANSMISSION OF CLASSIFIED AND/OR SENSITIVE UNCLASSIFIED U.S. GOVERNMENT INFORMATION IS REQUIRED. A COMSEC ACCOUNT WILL BE REQUIRED. GOVERNMENT WILL FURNISH EQUIPMENT FOR THE DURATION OF THIS CONTRACT.

ACCESS TO TOP SECRET INFORMATION IS REQUIRED IN THE PERFORMANCE OF THIS CONTRACT AND SHALL BE IN ACCORDANCE WITH DOD 5220.22-M, NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPO), CHAPTER 5. USER AGENCY APPROVAL IS REQUIRED PRIOR TO SUBCONTRACTING.

STORAGE OF TOP SECRET CLASSIFIED MATERIAL AT THE CONTRACTOR'S FACILITY IS NOT AUTHORIZED.

THE CONTRACTOR IS RESPONSIBLE FOR PROTECTION OF GOVERNMENT SENSITIVE DATA (AS DEFINED BY PUBLIC LAW 100-235) DURING THE PERIOD OF THIS AGREEMENT. SUCH PROTECTION WILL BE EQUIVALENT TO THE PROTECTION THE CONTRACTOR AFFORDS ITS OWN PROPRIETARY DATA AND TRADE SECRETS; BUT IN ANY EVENT, GOVERNMENT SENSITIVE DATA WILL NOT BE DISCUSSED, PROCESSED, OR TRANSMITTED OVER UNSECURE TELEPHONE, FACSIMILE, COMPUTER OR COMMUNICATIONS CIRCUITS.

ACCESS TO DOCUMENTS CONTAINING INTELLIGENCE INFORMATION IS REQUIRED IN THE PERFORMANCE OF THIS CONTRACT. ATTACHMENT #1, "SECURITY GUIDELINES FOR THE HANDLING OF INTELLIGENCE INFORMATION FOR CONTRACTORS" AND ATTACHMENT #2, DCID 1/7, "SECURITY CONTROLS ON THE DISSEMINATION OF INTELLIGENCE INFORMATION" PROVIDE GUIDANCE ON CONTROL OF INTELLIGENCE INFORMATION. USER AGENCY APPROVAL IS REQUIRED PRIOR TO SUBCONTRACTING.

THE FOLLOWING SECURITY CLASSIFICATION GUIDE(S) APPLIES AND WILL BE PROVIDED BY THE USER AGENCY AS REQUIRED:
OPNAVINST C5513.2B (63) "COMBAT SURVIVABILITY PROGRAM" AND OPNAVINST S5513.3B(28) "FUZES".

WHERE THE SECURITY CLASSIFICATION GUIDE (S) SPECIFIES A SPECIFIC DATE OR EVENT FOR DECLASSIFICATION, THE NEW DERIVATIVE CLASSIFICATION MARKINGS UNDER EXECUTIVE ORDER 12958 WILL APPLY.

DISTRIBUTION STATEMENTS MUST BE ON ALL CLASSIFIED AND UNCLASSIFIED TECHNICAL DOCUMENTS. REFER TO THE CONTRACT DATA REQUIREMENTS LIST (CDRL) BLOCK 9, FOR THE REQUIRED DISTRIBUTION STATEMENT FOR YOUR DATA, OR YOUR NAVAL AIR WARFARE CENTER WEAPONS DIVISION, CHINA LAKE, CA OR NAVAL AIR WEAPONS STATION CHINA LAKE, CA POINT OF CONTACT.

CLASSIFIED MATERIAL GENERATED UNDER THIS CONTRACT WILL BE MARKED WITH THE MOST RESTRICTIVE DOWNGRADING/DECLASSIFICATION INSTRUCTION APPLICABLE PROVIDED BY THE ATTACHED SECURITY CLASSIFICATION GUIDE (S) AND PER THE NEW DERIVATIVE CLASSIFICATION MARKINGS UNDER EXECUTIVE ORDER 12958.

DOCUMENTATION GENERATED AS A RESULT OF THIS CONTRACT WILL BE CLASSIFIED IN ACCORDANCE WITH SOURCE MATERIAL PROVIDED BY THE USER AND WILL CARRY THE MOST RESTRICTIVE DOWNGRADING/DECLASSIFICATION INSTRUCTIONS, WARNING NOTICES AND CONTROL MARKINGS APPLICABLE. A LISTING OF SOURCE MATERIAL WILL BE INCLUDED AS A PART OF THE DOCUMENT PREPARED BY THE CONTRACTOR.

PRIOR TO THE AUTHORIZATION OF DTIC SERVICES, CONTRACTORS MUST SUBMIT DD FORMS IN ACCORDANCE WITH REQUIREMENTS LISTED IN THE DOD 5220.22-M, NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPO), CHAPTER 11, SECTION 2.

AIS PROCESSING WILL BE CONDUCTED IN ACCORDANCE WITH THE NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPO), DEPARTMENT OF THE NAVY AUTOMATIC DATA PROCESSING SECURITY PROGRAM (OPNAVINST 5239.1A) AND APPROPRIATE LOCAL AIS INSTRUCTIONS.

TEMPEST SECURITY REQUIREMENTS ARE IMPOSED IF THIS CONTRACT REQUIRES THE CONTRACTOR TO ELECTRICALLY, ELECTRONICALLY, OR ELECTROMECHANICALLY PROCESS CLASSIFIED DATA AT THE SECRET - SPECIAL CATEGORY OR HIGHER LEVEL. UPON AWARD OF CONTRACT, THE ATTACHED CONTRACTOR TEMPEST QUESTIONNAIRE, ATTACHMENT #3, MUST BE COMPLETED BY THE CONTRACTOR AS PART OF THEIR CONTRACTUAL REQUIREMENTS. PUBLIC RELEASE IS NOT AUTHORIZED FOR TEMPEST SECURITY INFORMATION OR REQUIREMENTS. USER AGENCY APPROVAL IS REQUIRED PRIOR TO SUBCONTRACTING.

THE CONTRACTOR IS REQUIRED TO PROVIDE OPERATION SECURITY (OPSEC) PROTECTION FOR ALL CLASSIFIED INFORMATION (AS DEFINED BY FAR 4.401) AND SENSITIVE INFORMATION. IN ORDER TO MEET THIS REQUIREMENT, THE CONTRACTOR SHALL DEVELOP, IMPLEMENT AND MAINTAIN A FACILITY LEVEL OPSEC PROGRAM IN ACCORDANCE WITH ATTACHMENT #4, "OPERATIONS SECURITY GUIDANCE FOR CONTRACTORS" DATED AUGUST 1993, AND GUIDANCE PROVIDED. THE DEFENSE SECURITY SERVICE (DSS) WILL PERFORM OPSEC INSPECTIONS AS REQUIRED. PRIOR APPROVAL OF THE CONTRACTING ACTIVITY IS REQUIRED BEFORE IMPOSING OPSEC REQUIREMENTS ON A SUBCONTRACTOR.

THE "FOR OFFICIAL USE ONLY" INFORMATION PROVIDED UNDER THIS CONTRACT SHALL BE SAFEGUARDED IN ACCORDANCE WITH ATTACHMENT #5.

SECURITY REQUIREMENTS AND SECURITY AGREEMENTS FOR SHARED ACCESS OF SECURITY FUNCTIONS BETWEEN THE GOVERNMENT AND THIS CONTRACTOR HAVE BEEN ADDED TO THIS CONTRACT. SHARED ACCESS WILL BE APPROVED FOR INDIVIDUAL DELIVERY ORDERS.

SECURITY GUIDELINES FOR THE HANDLING OF INTELLIGENCE INFORMATION FOR CONTRACTORS:

1. Intelligence released to cleared DoD contractors, all reproductions thereof, and all other information generated based on, or incorporating data from, remain the property of the U.S. Government. The releasing command shall govern final disposition of intelligence information unless retention is authorized. Provide the Director, ONI (ONI-5) with a copy of the retention authorization.
2. Cleared DoD contractors shall not release intelligence to any of their components or employees not directly engaged in providing services under contract or other binding agreement or to another contractor (including subcontractors) without the consent of the releasing command.
3. Cleared DoD contractors who employ foreign nationals or immigrant aliens shall obtain approval from the Director, ONI (ONI-5) before releasing intelligence, regardless of their LAA.
4. See Attachment #., DCID 1/7, "Security Controls on the Dissemination of Intelligence Information", dated 30 JUNE 1998.

ATTACHMENT # / TO DD-254

DCID 1/7

Security Controls on the Dissemination of Intelligence Information

(Effective 30 June 1998)

Introduction

Pursuant to the provisions of the National Security Act of 1947, as amended, Executive Order 12333, Executive Order 12958 and implementing directives thereto, policies, controls, and procedures for the dissemination and use of intelligence information and related materials are herewith established in this Director of Central Intelligence Directive (Directive or DCID). Nothing in this policy is intended to amend, modify, or derogate the authorities of the DCI contained in Statute or Executive Order.

1.0 Policy

1.1 It is the policy of the DCI that intelligence be produced in a way that balances the need for maximum utility of the information to the intended recipient with protection of intelligence sources and methods. The controls and procedures established by this directive should be applied uniformly in the dissemination and use of intelligence originated by all Intelligence Community components in accordance with the following principles:

- 1.1.1 Originators of classified intelligence information should write for the consumer. This policy is intended to provide for the optimum dissemination of timely, tailored intelligence to consumers in a form that allows use of the information to support all need to know customers.
- 1.1.2 The originator of intelligence is responsible for determining the appropriate level of protection prescribed by classification and dissemination policy. Originators shall take a risk management approach when preparing information for dissemination.

2.0 Purpose

- 2.1 This Directive establishes policies, controls, and procedures for the dissemination and use of intelligence information to ensure that, while facilitating its interchange for intelligence purposes, it will be adequately protected. This Directive implements and amplifies applicable portions of the directives of the Information Security Oversight Office issued pursuant to Executive Order (E.O.) 12958 and directives of the Security Policy Board issued pursuant to E.O. 12958 and PDD-29.
- 2.2 Additionally, this Directive sets forth policies and procedures governing the release of intelligence to contractors and consultants, foreign governments, international organizations or coalition partners consisting of sovereign states, and to foreign nationals and immigrant aliens, including those employed by the US Government. pursuant to DCID 5/6, Intelligence Disclosure Policy.
- 2.3 Executive Order 12958 provides for the establishment of Special Access Programs, including Sensitive Compartmented Information. DCID 3/29 provides procedures for the establishment and review of Special Access Programs pertaining to intelligence activities and restricted collateral information. Intelligence Community components may establish and maintain dissemination controls on such information as approved under the policies and procedures contained in DCID 3/29, this DCID, and implementing guidance.

3.0 Definitions

- 3.1 "Caveated" information is information subject to one of the authorized control markings under Section 9.
- 3.2 Intelligence Community (and agencies within the Intelligence Community) refers to the United States Government agencies and organizations and activities identified in section 3 of the National Security Act of 1947, as amended, 50 USC 401a(4), and Section 3.4(f) (1 through 6) of Executive Order 12333.
- 3.3 Intelligence information and related materials (hereinafter referred to as "Intelligence") include the following information, whether written or in any other medium, classified pursuant to E.O. 12958 or any predecessor or successor Executive Order:
 - 3.3.1 Foreign intelligence and counterintelligence defined in the National Security Act of 1947, as amended, and in Executive Order 12333;
 - 3.3.2 Information describing US foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained through intelligence activities for exploitation and the results of the exploitation; and any other data resulting from US intelligence collection efforts; and,
 - 3.3.3 Information on Intelligence Community protective security programs (e.g., personnel, physical, technical, and information security).
- 3.4 "Need-to-know" is the determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. Such persons shall possess an appropriate security clearance and access approval granted pursuant to Executive Order 12968, Access to Classified Information.
- 3.5 Senior Official of the Intelligence Community (SOIC) is the head of an agency, office, bureau, or other intelligence element as identified in Section 3 of the National Security Act of 1947, as amended, 50 USC 401a(4), and Section 3.4(f) (1 through 6) of Executive Order 12333.
- 3.6 A "tear line" is the place on an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified and/or controlled report begins. The sanitized

sanitized version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with the "need to know" principle and foreign disclosure guidelines, of the information below the tear line.

4.0 General Applicability

- 4.1 In support of the Policy Statement in Section 1.0, classifiers of intelligence information shall take a risk management approach when preparing information for dissemination. In the interest of the widest possible dissemination of information to consumers with a "need to know", classifiers shall carefully consider the needs of all appropriate intelligence consumers regarding sources and methods information or sensitive analytic comments and use control markings only when necessary and in accordance with this directive, using tearlines and other formats to meet consumer needs for intelligence.
- 4.2 In carrying out this policy, intelligence producers shall prepare their reports and products at the lowest classification level commensurate with expected damage that could be caused by unauthorized disclosure. When necessary, the material should be prepared in other formats (e.g. tear-line form) to permit broader dissemination or release of information.
- 4.3 All material shall be portion marked to allow ready identification of information that cannot be broadly disseminated or released, except for material for which a waiver has been obtained under EO 12958.
- 4.4 The substance of this Directive shall be promulgated by each Intelligence Community component, and appropriate procedures permitting prompt interagency consultation established.

5.0 Use By and Dissemination Among Executive Branch Departments/Agencies of the US Government

5.1 Executive Order 12958 provides that classified information originating in one US department or agency shall not be disseminated beyond any recipient agency without the consent of the originating agency. However, to facilitate use and dissemination of intelligence within and among Intelligence Community components and to provide for the timely flow of intelligence to consumers, the following controlled relief to the "third agency rule" is hereby established:

5.1.1 Each Intelligence Community component consents to the use of its classified intelligence in classified intelligence products of other Intelligence Community components, including its contractors under Section 6, and to the dissemination of those products within executive branch departments/agencies of the US Government, except as specifically restricted by controls defined in this directive or other DCI guidance.

5.1.2 As provided in 5.1.1, classified intelligence that bears no restrictive control markings may be given secondary US dissemination in classified channels to any US executive branch department/agency not on original distribution if (a) the intelligence has first been sanitized by the removal of all references and inferences to intelligence sources and methods and the identity of the producing agency, or (b) if the product is not so sanitized, the consent of the originator has been obtained. If there is any doubt concerning a reference or inference to intelligence sources and methods, relevant intelligence documents should not be given secondary dissemination until the recipient has consulted with the originator.

5.1.3 Any component disseminating intelligence beyond the Intelligence Community assumes responsibility for ensuring that recipient organizations agree to observe the need-to-know principle and the restrictions prescribed by this directive, and to maintain adequate safeguards.

6.0 Policy and Procedures Governing the Release of Intelligence to Contractors and Consultants

6.1.1 SOICs, or their designees, may release intelligence to appropriately cleared or access-approved US contractors and consultants (hereinafter "contractor") having a demonstrated "need to know" without referral to the originating agency prior to release provided that:

6.1.1.1 At the initiation of the contract, the SOIC or her/his designee specifies and certifies in writing that disclosure of the specified information does not create an unfair competitive advantage for the contractor or a conflict of interest with the contractor's obligation to protect the information. If, during the course of the contract, the contractor's requirements for information changes to require new or significantly different information, the SOIC or his/her designee shall make a new specification and certification. In cases where the designated official cannot or does not resolve the issue of unfair competitive advantage or conflict of interest, consent of the originator is required;

6.1.1.2 Release is made only to contractors certified by the SOIC (or designee) of the sponsoring organization as performing classified services in support of a national security mission;

6.1.1.3 The contractor has an approved safeguarding capability if retention of the intelligence is required;

6.1.1.4 Contractors are not authorized to disclose further or release intelligence to any of their components or employees or to another contractor (including subcontractors) without the prior written notification and approval of the SOIC or his/her designee unless such

disclosure or release is authorized in writing at the initiation of the contract as an operational requirement;

- 6.1.1.5 Intelligence released to contractors, all reproductions thereof, and all other material generated based on, or incorporating data therefrom (including authorized reproductions), remain the property of the US Government. Final disposition of intelligence information shall be governed by the sponsoring agency;
- 6.1.1.6 National Intelligence Estimates (NIEs), Special National Intelligence Estimates (SNIIEs), and Interagency Intelligence Memoranda may be released to appropriately cleared contractors possessing an appropriate level facility clearance and need-to-know, except as regulated by provisions concerning proprietary information as defined in sections 6.1.1.7 and 9.3, below;
- 6.1.1.7 Except as provided in section 6.3 below, intelligence that bears the control marking "CAUTION-PROPRIETARY INFORMATION INVOLVED" (abbreviated "PROPIN" or "PR") may not be released to contractors, unless prior permission has been obtained from the originator and those providing the intelligence to the originator. Intelligence that bears the control marking, "Dissemination and Extraction of Information Controlled By Originator" (abbreviated "ORCON") may only be released to contractors within Government facilities. These control markings are further described under Sections 9.2 and 9.3, below; and
- 6.1.1.8 Authorized release to foreign nationals or foreign contractors is undertaken through established channels in accordance with sections 7 and 8, and DCID 5/6, Intelligence Disclosure Policy, and the National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (abbreviated title: National Disclosure Policy 1 or NDP 1) to the extent consistent with DCIDs and other DCI guidance.

6.2 Policies and Procedures for Contractors Inside Government Owned or Controlled Facilities

- 6.2.1 Contractors who perform duties inside a Government owned or controlled facility will follow the procedures and policies of that sponsoring Intelligence Community member in accordance with Section 6.1 of this directive

6.3 Policies and Procedures for Contractors Outside Government Owned or Controlled Facilities

- 6.3.1 Contractors who perform duties outside of Government owned or controlled facilities will adhere to the following additional policies and procedures:
 - 6.3.1.1 The SOIC of the sponsoring agency, or her/his designee, is responsible for ensuring that releases to contractors of intelligence marked ORCON and/or PROPIN are made only with the consent of the originating agency pursuant to this Directive and through established channels; (See Sections 9.2 and 9.3);
 - 6.3.1.2 The sponsoring agency shall maintain a record of material released;
 - 6.3.1.3 Contractors shall establish procedures to control all intelligence received, produced, and held by them in accordance with the provisions of the National Industrial Security Program Operating Manual. This will not impose internal receipt and document accountability requirements for internal traceability and audit purposes;
 - 6.3.1.4 All reproductions and extractions of intelligence shall be classified, marked, and controlled in the same manner as the original(s);
 - 6.3.1.5 Sensitive Compartmented Information released to contractors shall be controlled pursuant to the provisions of DCID 1/19, Security Policy for Sensitive Compartmented Information (SCD); and,
 - 6.3.1.6 Sponsoring agencies shall delete any reference to the Central Intelligence Agency, the

phrase "Directorate of Operations" and any of its components, the place acquired, the field number, the source description, and field dissemination from all CIA Directorate of Operations reports passed to contractors, unless prior approval to do otherwise is obtained from CIA.

7.0 Release to Foreign Governments, International Organizations, and Coalition Partners

- 7.1 It is the policy of the DCI that intelligence may be shared with foreign governments, and international organizations or coalition partners consisting of sovereign states to the extent such sharing promotes the interests of the United States, is consistent with US law, does not pose unreasonable risk to US foreign policy or national defense, and is limited to a specific purpose and normally of limited duration. The release of intelligence to such entities is subject to this Directive, DCID 5/6, Intelligence Disclosure Policy, and NDP 1 to the extent consistent with DCIDs and other DCI guidance.
 - 7.1.1 Intelligence Community elements shall restrict the information subject to control markings to the minimum necessary. If it is not possible to prepare the entire report at the collateral, unclassified level, IC elements shall organize their intelligence reports and products to identify clearly information not authorized for release to foreign entities.
- 7.2 Intelligence information that bears no specific control marking may be released to foreign governments, international organizations, or coalition partners provided that:
 - 7.2.1 A positive foreign disclosure decision is made by a Designated Intelligence Disclosure Official in accordance with procedures in DCID 5/6;
 - 7.2.2 No reference is made to the originating agency or to the source of the documents on which the released product is based; and,
 - 7.2.3 The source or manner of acquisition of the intelligence (including analytic judgments or techniques), and/or the location where the intelligence was collected (if relevant to protect sources and methods) is not revealed and cannot be deduced in any manner.
- 7.3 RESTRICTED DATA and FORMERLY RESTRICTED DATA may only be released to foreign governments pursuant to an agreement for cooperation as required by Sections 123 and 144 of Public Law 585, Atomic Energy Act of 1954, as amended.

8.0 Dissemination to Non-Governmental Foreign Nationals or Foreign Contractors

- 8.1 It is the policy of the DCI that no classified intelligence will be shared with foreign nationals, foreign contractors, or international organizations not consisting of sovereign states, except in accordance with the provisions of this Section.
- 8.2 Intelligence, even though it bears no restrictive control markings, will not be released in any form to foreign nationals or immigrant aliens (including those employed by, used by, or integrated into the US Government) without the permission of the originator. In such cases where permission of the originator has been granted, the release must be in accordance with DCID 5/6, and the NDP 1 to the extent consistent with DCIDs and other DCI guidance.
- 8.3 Release of intelligence to a foreign contractor or company under contract to the US Government must be through the foreign government of the country which the contractor is representing, unless otherwise directed in government-to-government agreements or there is an appropriate US channel for release of the information. Provisions concerning release to foreign governments is contained in Section 7.0, above.

9.0 Authorized Control Markings

- 9.1 DCI policy is that the authorized control markings for intelligence information in this Section shall be individually assigned as prescribed by an Original Classification Authority (OCA) or by officials designated by a SOIC and used in conjunction with security classifications and other markings specified by Executive Order 12958 and its implementing directive(s). Unless originator consent is obtained, these markings shall be carried forward to any new format or medium in which the same information is incorporated.
- 9.1.1 To the maximum extent possible, information assigned an authorized control marking shall not be combined with uncaveated information in such a way as to render the uncaveated information subject to the control marking. To fulfill the requirements of paragraph 9.6.1 below, SOICs shall establish procedures in implementing directives to expedite further dissemination of essential intelligence. Whenever possible, caveated intelligence information reports should include the identity and contact instructions of the organization authorized to approve further dissemination on a case-by-case basis.
- 9.2 "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR" (ORCON)
- 9.2.1 This marking (ORCON or abbreviated OC) may be used only on classified intelligence that clearly identifies or would reasonably permit ready identification of intelligence sources or methods that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness. It is used to enable the originator to maintain continuing knowledge and supervision of distribution of the intelligence beyond its original dissemination. This control marking may not be used when access to the intelligence information will reasonably be protected by use of its classification markings, i.e., CONFIDENTIAL, SECRET or TOP SECRET, or by use of any other control markings specified herein or in other DCIDs. Requests for further dissemination of intelligence bearing this marking shall be reviewed in a timely manner.
- 9.2.2 Information bearing this marking may be disseminated within the headquarters² and specified subordinate elements of recipient organizations, including their contractors within Government facilities. This information may also be incorporated in whole or in part into other briefings or products, provided the briefing or intelligence product is presented or distributed only to original recipients of the information. Dissemination beyond headquarters and specified

subordinate elements or to agencies other than the original recipients requires advance permission from the originator.

9.2.3 Information bearing this marking must not be used in taking investigative or legal action without the advance permission of the originator.

9.2.4 As ORCON is the most restrictive marking herein, agencies that originate intelligence will follow the procedures established in the classified DCID 1/7 Supplement, "Guidelines for Use of ORCON Caveat."

9.3 "CAUTION-PROPRIETARY INFORMATION INVOLVED" (PROPIN). This marking is used, with or without a security classification, to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value³. This marking may be used on government proprietary information only when the government proprietary information can provide a contractor(s) an unfair advantage, such as US Government budget or financial information. Information bearing this marking shall not be disseminated outside the Federal Government in any form without the express permission of the originator of the intelligence and provider of the proprietary information. This marking precludes dissemination to contractors irrespective of their status to, or within, the US Government without the authorization of the originator of the intelligence and provider of the information. This marking shall be abbreviated "PROPIN" or "PR."

9.4 "NOT RELEASABLE TO FOREIGN NATIONALS" - NOFORN (NF). This marking is used to identify intelligence which an originator has determined falls under the criteria of DCID 5/6, "Intelligence Which May Not Be Disclosed or Released," and may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval.

9.5 "AUTHORIZED FOR RELEASE TO..(name of country(ies)/international organization)" (REL TO). This control marking is used when a limited exception to the marking requirements in Section 9.4 may be authorized to release the information beyond US recipients. This marking is authorized only when the originator has an intelligence sharing arrangement or relationship with a foreign government approved in accordance with DCI policies and procedures that permits the release of the specific intelligence information to that foreign government, but to no other in any form without originator consent.

9.6 Further Dissemination of Intelligence with Authorized Control Marking(s)

9.6.1 This Directive does not restrict an authorized recipient of intelligence at any level from directly contacting the originator of the intelligence to ask for relief from a specific control marking(s) in order to further disseminate intelligence material to additional users for which the authorized original recipient believes there is a valid need-to-know. Authorized recipients are encouraged to seek such further dissemination through normal liaison channels for release to US Government agencies or contractors and through foreign disclosure channels for foreign release, on a case-by-case basis, in order to expedite further dissemination of essential intelligence.

9.6.2 Authorized recipients may obtain information regarding points of contact at agencies that originate intelligence from their local dissemination authorities or from instructions issued periodically by these intelligence producers. Intelligence products often also carry a point of contact name/office and telephone number responsible for the product. If no other information is available, authorized recipients are encouraged to contact the producing agency of the document to identify the official or office authorized to provide relief from authorized control marking(s).

9.6.3 If there are any questions about whom to contact for guidance, recipients are also encouraged

to contact the Director of Central Intelligence (DCI) representative at the Commander-in-Chief (CINC) Headquarters, overseas mission, trade delegation, or treaty negotiating team under which they operate.

- 9.7 A SOIC may authorize the use of additional security control markings for Sensitive Compartmented Information (SCI), Special Access Program (SAP) information, restricted collateral information, or other classified intelligence information, consistent with policies and procedures contained in DCID 3/29 and this directive. A uniform list of security control markings authorized for dissemination of classified information by components of the Intelligence Community, and the authorized abbreviated forms of such markings, shall be compiled in the central register maintained pursuant to DCID 3/29. The forms of the markings and abbreviations listed in this register shall be the only forms of those markings used for dissemination of classified information by components of the Intelligence Community, unless an exception is specifically authorized by a SOIC.

10.0 Dissemination and Disclosure Under Emergency Conditions

- 10.1 Certain emergency situations⁴ that involve an imminent threat to life or mission warrant dissemination of intelligence to organizations and individuals not routinely included in such dissemination. When the national command authority (NCA) directs that an emergency situation exists, SOICs will ensure that intelligence support provided to the ongoing operations conforms with this Directive, DCID 5/6, and NDP 1 to the maximum extent practical and consistent with the mission.

10.1.2 Dissemination of intelligence under this provision is authorized only if: (a) an authority designated by the military commander or civilian official determines that adherence to this DCID reasonably is expected to preclude timely dissemination to protect life or mission; (b) disseminations are for limited duration and narrowly limited to persons or entities that need the information within 72 hours to satisfy an imminent emergency need; and (c) there is insufficient time to obtain approval through normal intelligence disclosure channels.

10.1.3 The disclosing authority will report the dissemination through normal disclosure channels within 24 hours of the dissemination, or at the earliest opportunity thereafter as the emergency permits. For purposes of this provision, planning for contingency activities or operations not expected to occur within 72 hours does not constitute "imminent" need that warrants exercise of the emergency waiver to bypass the requirements of this DCID.

10.1.4 Military commanders and/or responsible civilian officials will ensure that written guidelines for emergency dissemination contain provisions for safeguarding disseminated intelligence and notifying producers of disclosures of information necessary to meet mission requirements.

10.1.5 The NCA, and/or major commands or responsible civilian officials will immediately advise intelligence producers when the emergency situation ends.

11.0 Procedures Governing Use of Authorized Control Markings

- 11.1 Any recipient desiring to disseminate intelligence in a manner contrary to the control markings established by this Directive must obtain the advance permission of the agency that originated the intelligence. Such permission applies only to the specific purpose agreed to by the originator and does not automatically apply to all recipients. Producers of intelligence will ensure that prompt consideration is given to recipients' requests 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 marking(s).
- 11.2 The control markings authorized above shall be shown on the title page, front cover, and other applicable pages of documents; incorporated in the text of electrical communications; shown on graphics; and associated (in full or abbreviated form) with data stored or processed in automated information systems. The control markings also shall be indicated by parenthetical use of the marking abbreviations at the beginning or end of the appropriate portions in accordance with E.O. 12958.

12.0 Obsolete Restrictions and Control Markings

- 12.1 The following control markings are obsolete and will not be used in accordance with the following guidelines:
- 12.1.1 **WNINTEL** and **NOCONTRACT**. The control markings, Warning Notice - Intelligence Sources or Methods Involved (**WNINTEL**), and **NOT RELEASABLE TO CONTRACTORS/CONSULTANTS** (abbreviated **NOCONTRACT** or **NC**) were rendered obsolete effective 12 April 1995. No permission of the originator is required to release, in accordance with this Directive, material marked **WNINTEL**. Holders of documents prior to 12 April 1995 bearing the **NOCONTRACT** marking should apply the policies and procedures contained in Section 6.1 for possible release of such documents.
- 12.1.2 Remarking of material bearing the **WNINTEL**, or **NOCONTRACT**, control marking is not required; however, holders of material bearing these markings may line through or otherwise remove the marking(s) from documents or other material.
- 12.1.3 Other obsolete markings include: **WARNING NOTICE-INTELLIGENCE SOURCES OR METHODS INVOLVED**, **WARNING NOTICE-SENSITIVE SOURCES AND METHODS INVOLVED**, **WARNING NOTICE-INTELLIGENCE SOURCES AND METHODS INVOLVED**, **WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED**, **CONTROLLED DISSEM**, **NSC PARTICIPATING AGENCIES ONLY**, **INTEL COMPONENTS ONLY**, **LIMITED**, **CONTINUED CONTROL**, **NO DISSEM ABROAD**, **BACKGROUND USE ONLY**, **USIB ONLY**, **NFIB ONLY**.
- 12.2 Questions with respect to current applications of all control markings authorized by earlier Directives on the dissemination and control of intelligence and used on documents issued prior to the effective date of this Directive should be referred to the agency or department originating the intelligence so marked.

13.0 Reporting Unauthorized Disclosures

- 13.1 Violations of the foregoing restrictions and control markings that result in unauthorized disclosure by one agency of the intelligence of another shall be reported to the Director of Central Intelligence through appropriate Intelligence Community channels.

14.0 Responsibilities of SOICs

- 14.1 SOICs shall be responsible for the implementation of internal controls and shall conduct training to ensure that the dissemination and release policies contained in this Directive and the limitations on the use of control markings are followed. SOICs shall assure that agency personnel are accountable for the proper marking of classified information under this Directive and Section 5.6 of EO 12958.
- 14.2 SOICs shall establish challenge procedures by which US consumers may register complaints about the misuse of control markings or the lack of use of tear line reporting or portion marking. Information concerning such challenges shall be provided to the Security Policy Board staff upon request or for the annual review.

15.0 Annual Report on the Use of Control Markings

- 15.1 The Security Policy Board staff shall report to the DCI and Deputy Secretary of Defense on Intelligence Community compliance with this Directive, including recommendations for further policies in this area. The report will include an in-depth evaluation of the use of control markings in intelligence reporting/production, including consumer evaluations and producer perspectives on implementation of the Directive. The report shall also include information and statistics on challenges formally lodged pursuant to agency procedures under section 1.9 of Executive Order 12958 within and among intelligence agencies on the use of control markings, including their adjudication and the number of times the authority in Section 10 was used and the documents provided. In order to inform the Security Policy Board staff of substantive detail in these areas for purposes of this review, Intelligence Community elements shall respond to requests for information from the Security Policy Board staff. Intelligence Community elements may build this program into their Self-Inspection programs under E.O. 12958. The Security Policy Board staff shall also obtain pertinent information on this subject from intelligence consumers as required.
- 15.2 The report required by this Section shall be conducted annually, unless otherwise directed by the DCI. The Staff Director, Security Policy Board shall establish the schedule for the report.

16.0 Interpretation

- 16.1 Questions concerning the implementation of this policy and these procedures shall be referred to the Community Management Staff.

Signed by George D. Tenet

30 June 1998

Director of Central Intelligence

Date

Footnotes:

- 1 This Directive supersedes DCID 1/7, dated 12 April 1995
 - 2 Recipients will apprise originating agencies as to which components comprise the headquarters element and identify subordinate elements that may be included as direct recipients of intelligence information.
 - 3 This provision is a requirement of the Trade Secrets Act, as amended (18 USC 1905). The consent of the originator is required to permit release of material marked CAUTION-PROPRIETARY INFORMATION INVOLVED, PROPIN or PR to other than federal government employees.
 - 4 For the purposes of implementing this portion of the DCID, "emergency situation" is defined as one of the following:
 - a. declared Joint Chiefs of Staff (JCS) alert condition of defense emergency, air defense emergency or DEFCON 3;
 - b. hostile action(s) being initiated against the United States or combined US/coalition/friendly forces;
 - c. US persons or facilities being immediately threatened by hostile forces;
 - d. US or combined US/coalition/friendly forces planning for or being deployed to protect or rescue US persons, or US/coalition/friendly forces;
 - e. US civilian operations in response to US or international disasters/catastrophes of sufficient severity to warrant Presidential declared disaster assistance/relief.
-

Note:

DCID 1/7 must be marked CONFIDENTIAL//NOFORN//X1 when attached to the text of the DCID 1/7 Supplement.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

CONTRACTOR TEMPEST QUESTIONNAIRE

1. The following TEMPEST questionnaire must be completed and sent to the contracting authority and the Certified TEMPEST Technical Authority within 30 days after contract has been awarded to CONTRACTORS who will be processing National Security Information at the SECRET - SPECIAL CATEGORY or higher level. This is an information collection questionnaire only. This is not a directive, implied requirement or an encouragement to procure TEMPEST equipment or shielding for use on this contract. DO NOT procure TEMPEST equipment unless specifically directed by the contracting authority.

a. Please answer the following questions promptly and return the information to the contracting authority and to the Certified TEMPEST Technical Authority listed below:

Department of the Navy
Code 723AF
SPAWARSYSCEN
P. O. Box 190022
North Charleston, SC 29419-9022

1. What is the highest classification level of material to be processed/handled by electronic or electromechanical automated information processing equipment?
2. What special categories of classified material (Sensitive Compartmented Information, Nuclear Command and Control, Special Access Program, Single Integrated Operational Plan, etc.) are processed?
3. What is the approximate percentage of processing time for Top Secret and Special Category information compared to the total processing time?
4. Provide the specific location, address and zip code, where the classified processing will be performed.
5. Provide facility information, are there other tenants, other tenant's names, type of business (govt., commercial, foreign commercial, foreign govt., etc.).
6. Provide the name, address, position title and phone number at the facility where classified processing will occur, a point of contact who is knowledgeable of the processing requirement, the types of equipment to be used and the physical layout of the facility.
7. Perishability of Information Processed - Identify if the information being processed is of long term value (e.g. strategic) or short term value (e.g. tactical).
8. Physical Control - Describe the physical/access control over the facility and areas containing the system under review. This includes guards (number, hours of posting, patrols, etc.); badging; control over access to facility; alarms; procedures to monitor/control uncleared or unauthorized personnel including maintenance force, vending personnel, and telephone/power maintainers/installers. Determine the level of authority which exists for the inspection or removal of personnel who could potentially exploit TEMPEST vulnerabilities. Examine the posting of warning signs and the implementation of procedures in effect to exercise control over parking and other areas adjacent to or in close proximity to the facility/system under review.
9. TEMPEST Profile of Equipment - Provide generic or actual TEMPEST profile information for each equipment/system used to process classified information at the facility. Identify existing on-site TEMPEST test results for the facility including zoning tests.

b. Is this company foreign owned or controlled? If so what is the country?

c. Provide contract number and identify sponsoring command.

2. Additional information:

a. Prime contractors cannot pass TEMPEST requirements to subcontractors. Subcontractors must submit a Contractor TEMPEST Questionnaire prior to processing.

b. Interim processing for Top Secret Non Special Category and below is allowed once the contractor's TEMPEST Countermeasure Review is received.

c. TEMPEST Countermeasure Reviews for awarded contracts should be mailed return receipt requested to:

Department of the Navy
Code 723AF
SPAWARSYSCEN
P. O. Box 190022
North Charleston, SC 29419-9022

d. Provide the local TEMPEST Control Officer with copy of countermeasure results.

e. For questions concerning the completion of this form contract Mr. Andy Fisher at (803) 974-6785, DSN 563-2030 extension 6785, at SPAWARSYSCEN.

**OPERATIONS SECURITY
GUIDANCE
FOR
CONTRACTORS**

AUGUST 1993

**PREPARED BY:
OPERATIONS SECURITY OFFICE
SAFETY AND SECURITY DEPARTMENT
NAVAL AIR WEAPONS STATION
CHINA LAKE, CALIFORNIA 93555-6001
and
Point Mugu, California 93042-5000**

ATTACHMENT 4 TO DD FORM 254
OF 7-11-2001

OPERATIONS SECURITY GUIDANCE FOR CONTRACTORS

DEFINITION

Operations security, or OPSEC, is the process of denying adversaries information about friendly [our] capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities. OPSEC applies and should be emphasized at all levels of management down to the lowest shop and office level. Essentially, OPSEC has two objectives:

1. Protecting friendly operations
2. Degrading an adversary's war fighting capabilities through denial or control of information essential for planning and decision making.

BACKGROUND

One of the prime objectives of the U.S. intelligence community is the early acquisition of critical information regarding the research, development, testing, and evaluation (RD&E) of adversarial military weapon systems and associated hardware. Conversely, there is no doubt that this nations potential adversaries are also very interested in our own development of military systems.

1. The reason for this mutual interest derives from the basic objectives of military intelligence: to avoid being surprised on the battlefield, while at the same time having the ability to render an adversary helpless through the element of surprise.

2. To avoid being surprised on the battlefield, it is of utmost importance to have prior knowledge of weapons the adversary might use, their capabilities, methods of employment and susceptibility to countermeasures and countertactics. It is imperative that this information be acquired as early as possible, thus making the development and initial testing phases of a weapon system a prime target for intelligence collection.

The purpose of this foreign intelligence effort is to determine general developmental trends of future U.S. weaponry, to obtain hard-core parametric data about specific weapons in order to devise countermeasures, and to acquire advanced technology that could possibly reduce developmental time and money associated with a country's own military hardware programs.

With this emphasis, it is easy to understand why our potential adversaries are most interested in the work and results of the Department of Defense and its contractors.

Experience from the early days of Vietnam and the original OPSEC effort (code-named Purple Dragon) demonstrated that something other than the traditional security programs (information, personnel, physical and industrial security) was required to maintain this element of surprise and to deter foreign intelligence collection efforts. This has developed the OPSEC concept which, unlike conventional security programs, focuses on identifying and protecting the specific information needed by an adversary to undermine the effectiveness of a specific operation or weapon system.

OPSEC is not designed to replace traditional security programs. Traditional security programs are aimed at the protection of classified information, while OPSEC is aimed at the protection of *indicators*, classified or unclassified, that reveal *U.S. capabilities or intentions*.

Evaluations of peacetime and crisis deployments; exercises, reconnaissance, systems acquisition tests, personnel, logistics and security functions; test ranges, laboratories, and other activities, revealed the need to apply OPSEC to RDT&E activities as well as combat operations.

INDICATORS

Unless an adversary has access to planning actions by means of espionage that exploit classified information, he must depend on intelligence derived from detectable activities.

1. Detectable activities include any emission or reflection of energy, any action, or anything that can be easily observed or recorded, and all material available to the public. Detectable activities are defined as activities incident to routine operations that convey information to our adversaries.

2. When detectable activities are observed, photographed or "detected" by human or technical means, they may provide our adversaries with sufficient information to reach conclusions approximating classified information about our intentions and capabilities. This enables our adversaries to make effective planning decisions.

3. Routinely, detectable activities are harmless; however, when the information revealed is essential to the needs of the adversary, it may compromise our end product and negate our efforts. These harmful detectable activities are known as indicators and observables.

a. An indicator is any item of information which reflects an intention or capability. Indicators are obtained from documentation such as supply stubs, personnel records, test schedules, test plans, OPSEC plans, required operational capabilities, program introductions, mission statements, test evaluations, etc.

b. An observable is an activity or anything (such as equipment, technical documents, etc.) that can be observed or photographed by human agents or any of the multidisciplinary technical intelligence collection methods such as the interception and analysis of compromising computer emanations, radio and telephone communications, radar emissions, and other intentional and unintentional electronic emissions, as well as technical imaging techniques such as photography, infrared photography, and radar imagery.

PROCESS

OPSEC is the process used in the RDT&E community to maintain the element of surprise regarding the development of U.S. weapons systems. OPSEC, as applied to weapons systems development, is the identification, control and protection of the specific essential information needed by an adversary to develop countermeasures and countertactics, or that which could be crucial in the transfer of technology. The essential information that must be protected need not be classified and is usually viewed as unimportant when examined in isolation.

OPSEC is a systematic process designed to be an integral part of overall planning.

1. OPSEC planners must first establish an OPSEC team composed of employees from various areas. The reason for the team approach is that OPSEC analysis requires close coordination between management, security specialists, and subject matter experts.
2. The key to the OPSEC concept is the identification of the information that requires protection. This information is called Essential Elements of Friendly [our] Information or EEFI and may be corporate proprietary data, classified information, privacy data, For Official Use Only material, or unclassified, but national security-sensitive, information.
3. When identifying EEFI, the team should include those items of information which when put together, would give either a piece or all of the essential information. This step is necessary because an adversary, like a puzzle enthusiast, does not need all the pieces to accurately guess what the picture is.
4. Next the team must identify the threat to that information by creating a composite profile of their adversary's intelligence collection capabilities.
5. Chronologically identifying all activities involving the essential information is the next step. All activity, including supporting activities that might reveal essential information, must be reviewed. It is important to ensure the sequence of events is exactly how the operation really works rather, than how management plans for it to work.
6. Each event in which sensitive information appears is an opportunity for an adversary to exploit, and is considered an OPSEC vulnerability.
7. It is imperative to assume the adversary's point of view during the OPSEC process; in order to know what our adversaries see, we must look at our operations with their eyes. Additionally, from a fiscal point of view, if an adversary cannot exploit a vulnerability because of the limitations in his intelligence collection capabilities, then no countermeasures are required. On the other hand, if the adversary has the capability to exploit a vulnerability, then countermeasures are warranted.
8. Finally, the OPSEC team should prioritize the vulnerabilities from the most to the least serious. Then the team can select countermeasures most effectively, using such factors as cost, ease of implementation, and number of vulnerabilities reduced.
9. Two concepts the OPSEC team should consider when developing countermeasures are:

- a. Vulnerabilities can often be minimized but rarely eliminated
- b. The objective of the OPSEC program is to make collection sufficiently difficult to persuade the adversary to collect information somewhere else.

SPECIAL CONSIDERATIONS

Normally, contractors activities do not in and of themselves, generate a great deal of sensitive information or EEFI; however, contractor facilities, equipment and employees are used to store, transmit and process classified information, unclassified but national security-sensitive information, and EEFI which was generated outside their facilities.

Contractor activities usually have little intrinsic intelligence value until associated with a specific weapon system or activity. Unclassified, non-proprietary, For Official Use only, and privacy data are not generally national security-related issues; however, this type of information, when merged with information pertaining to specific weapons or weapons systems, may become sensitive or even classified. Therefore, it is incumbent upon all contractors to ascertain the sensitivity of information before introducing the information into their facilities.

Operations and activities can be roughly divided into two categories with respect to OPSEC: work performed inside workspaces and work performed outside workspaces.

1. Inside workspaces OPSEC is covered by traditional security programs. Protecting information whether contained in computers, on written documents, or in communications networks is a matter of complying with information, personnel, and physical security procedures. The essence of OPSEC inside work spaces is identifying the information you need to protect, establishing minimum procedures for protecting that information, and communicating this to employees.

The sensitivity of information received by (as opposed to generated by) the facility from external sources must be determined and appropriately communicated to employees at the time this information is received at the facility.

2. Whenever work is performed outside workspaces, or whenever EEFI is released from your workspaces (to other workspaces in or out of your facility) for whatever reason, an OPSEC determination is necessary: will the activities unnecessarily expose sensitive information, and what can be done to counter this exposure? This analysis must then be documented in the form of an OPSEC plan. The OPSEC plan must address five issues:

- a. The activity that involves the sensitive information
- b. The sensitive information that might be exposed
- c. The threat to that information
- d. Where the information is vulnerable or what is it about the activity that exposes this information
- e. What countermeasures can be applied to reduce or eliminate these vulnerabilities.

"FOR OFFICIAL USE ONLY" INFORMATION

The "For Official Use Only" (FOUO) marking is assigned to information at the time of its creation in 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.

Other non-security markings, such as "Limited Official Use" and "Official Use Only" are used by non-DoD User Agencies for the same type of information and should be safeguarded and handled in accordance with instruction received from such agencies.

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 to it.

Identification Markings. An unclassified document containing FOUO information will be marked "For Official Use Only" at the bottom of the front cover (if any), on the first page, on each page containing FOUO information, on the back page, and on the outside of the back cover (if any). No portion markings will be shown. Within a classified document, an individual page contains both FOUO 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 FOUO information but no classified information, the portion will be marked, "FOUO."

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

Dissemination. Contractors may disseminate "For Official Use Only" information to their employees and subcontractors who have a need for the information in connection with a classified contract.

Storage. During working hours, "For Official Use Only" information 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 nonworking 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 nonworking hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection or the material can be stored in locked receptacles such as file cabinets, desks, or bookcases.

Transmission. "For Official Use Only" information may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail.

Disposition. When no longer needed, FOUO information may be disposed of by tearing each copy into pieces to preclude reconstructing, and placing it in a regular trash container or as directed by the User Agency.

Unauthorized Disclosure. Unauthorized disclosure of "For Official Use Only" information does not constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT				1. CONTRACT ID CODE	PAGE OF PAGES 1 2
2. AMENDMENT/MODIFICATION NO. P00002		3. EFFECTIVE DATE 31-Oct-2001	4. REQUISITION/PURCHASE REQ. NO. N60530-0290-CYBC		5. PROJECT NO.(If applicable)
6. ISSUED BY CDR NAWCWD CODE 210000D ATTN: S. LAMBERT (760) 939-7652 1 ADMIN CIR, BLDG 982 CHINA LAKE CA 93555-6100		CODE N68936	7. ADMINISTERED BY (If other than item 6) DCM BALTIMORE 217 E. REDWOOD, SUITE 1800 BALTIMORE MD 21202-5299		CODE S2101A
8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and Zip Code) THE SURVICE ENGINEERING COMPANY JAMES B. FOULK SURVICE ENGINEERING COMPANY 4695 MILLENNIUM DRIVE BELCAMP MD 21017				9A. AMENDMENT OF SOLICITATION NO.	
				9B. DATED (SEE ITEM 11)	
				X 10A. MOD. OF CONTRACT/ORDER NO. N68936-01-D-0037	
				X 10B. DATED (SEE ITEM 13) 26-Jul-2001	
CODE 7T988		FACILITY CODE			
11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS					
<input type="checkbox"/> The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offer <input type="checkbox"/> is extended, <input type="checkbox"/> is not extended. Offer must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.					
12. ACCOUNTING AND APPROPRIATION DATA (If required)					
13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.					
A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.					
B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(B).					
C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:					
X D. OTHER (Specify type of modification and authority) mutual agreement of both parties.					
E. IMPORTANT: Contractor <input type="checkbox"/> is not, <input checked="" type="checkbox"/> is required to sign this document and return <u>1</u> copies to the issuing office.					
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.) See pages herein					
<small>Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.</small>					
15A. NAME AND TITLE OF SIGNER (Type or print)			16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) MAUREENA R MUELLER / CONTRACTING OFFICER		
15B. CONTRACTOR/OFFEROR		15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY 		16C. DATE SIGNED 31-Oct-2001
(Signature of person authorized to sign)			(Signature of Contracting Officer)		

EXCEPTION TO SF 30
APPROVED BY OIRM 11-84

30-105-04

STANDARD FORM 30 (Rev. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

SECTION SF 30 BLOCK 14 CONTINUATION PAGE

SUMMARY OF CHANGES

Changes in Solicitation/Contract/Order Form

The contractor organization has changed from
THE SURVICE ENGINEERING COMPANY
SURVICE ENGINEERING COMPANY
1003 OLD PHILADELPHIA ROAD
SUITE 103
ABERDEEN, MD 21001-4011
to
THE SURVICE ENGINEERING COMPANY
SURVICE ENGINEERING COMPANY
4695 MILLENNIUM DRIVE
BELCAMP, MD 21017

Changes in Section B

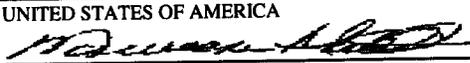
The following clauses which are incorporated by full text have been added or modified:

B-NSTD-07 PAYMENT OF FIXED FEE

Subject to the withholding provisions of the clause at FAR 52.216-8, Fixed Fee, the fixed fee specified shall be paid at the rate of 6(4) per direct labor hour for the prime contractor and core subcontractor(s) listed below expended during each vouchering period; provided, however, that the total fee payable shall not exceed the fee established in the delivery orders or the contract, whichever is lower.

Prime: SURVICE Engineering Company

Core Subcontractors: SRS Technologies
Computer Sciences Corporation

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT				1. CONTRACT ID CODE	PAGE OF PAGES	
				1	3	
2. AMENDMENT/MODIFICATION NO. P00003	3. EFFECTIVE DATE 15-Nov-2002	4. REQUISITION/PURCHASE REQ. NO. N60530-0290-CYBC		5. PROJECT NO.(If applicable)		
6. ISSUED BY CDR NAWCWD CODE 210000D ATTN: L. FLETCHER 1 ADMIN CIR, BLDG 2483 CHINA LAKE CA 93555-8100		CODE N68936	7. ADMINISTERED BY (If other than item 6) DCM BALTIMORE 217 E. REDWOOD, SUITE 1800 BALTIMORE MD 21202-5299		CODE S2101A	
8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and Zip Code) THE SURVICE ENGINEERING COMPANY JAMES B. FOULK SURVICE ENGINEERING COMPANY 4695 MILLENNIUM DRIVE BELCAMP MD 21017				9A. AMENDMENT OF SOLICITATION NO.		
				9B. DATED (SEE ITEM 11)		
				X	10A. MOD. OF CONTRACT/ORDER NO. N68936-01-D-0037	
				X	10B. DATED (SEE ITEM 13) 26-Jul-2001	
CODE 7T988	FACILITY CODE		11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS			
<input type="checkbox"/> The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offer <input type="checkbox"/> is extended, <input type="checkbox"/> is not extended.						
<p>Offer must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods:</p> <p>(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.</p>						
12. ACCOUNTING AND APPROPRIATION DATA (If required) See Schedule						
13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.						
A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.						
X B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(B).						
C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:						
D. OTHER (Specify type of modification and authority)						
E. IMPORTANT: Contractor <input checked="" type="checkbox"/> is not, <input type="checkbox"/> is required to sign this document and return _____ copies to the issuing office.						
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)						
- SEE HEREIN -						
Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.						
15A. NAME AND TITLE OF SIGNER (Type or print)			16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)			
			MAUREENA R MUELLER / CONTRACTING OFFICER			
15B. CONTRACTOR/OFFEROR		15C. DATE SIGNED	16B. UNITED STATES OF AMERICA		16C. DATE SIGNED	
_____ (Signature of person authorized to sign)			BY  (Signature of Contracting Officer)		15-Nov-2002	

EXCEPTION TO SF 30
APPROVED BY OIRM 11-84

30-105-04

STANDARD FORM 30 (Rev. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

SECTION SF 30 BLOCK 14 CONTINUATION PAGE

SUMMARY OF CHANGES

Changes in Section G

Summary for the Payment Office

As a result of this modification, the total funded amount of the contract is decreased by \$500,000.00 from \$500,000.00 to \$0.00

CLIN :0001

AA: 97X4930 NH2C 000 77777 0 068936 2F 000000 000290CYBC00
is decreased by \$500,000.00 from \$500,000.00 to \$0.00

Changes in Section H

The following clause which is incorporated by full text has been modified:

H-TXT-02 DESIGNATION OF CONTRACTING OFFICER'S REPRESENTATIVE

(a) The Contracting Officer has designated:

NAME: Jim Tucker
CODE: 418100D
ADDRESS: Commander, NAWCWD
1 Administration Circle
China Lake, CA 93555-6100

TELEPHONE NO. 760/939-8442

as the authorized Contracting Officer's Representative (COR) for this contract/order and

NAME: Martha L. Hoppus
CODE: 418100D
ADDRESS: Commander, NAWCWD
1 Administration Circle
China Lake, CA 93555-6100

TELEPHONE NO. 760/939-8424

as the authorized Alternate Contracting Officer's Representative (ACOR) for this contract order.

(b) The COR is responsible for monitoring the performance and progress, as well as overall technical management of the orders placed hereunder and should be contacted regarding any questions or problems of a technical nature. In no event, however, will any understanding or agreement, modification, change order, or other matter deviating from the terms of the contract between the Contractor and any person other than the Contracting Officer be effective or binding upon the Government, unless formalized by proper contractual documents executed by the Contracting Officer prior to the completion of this contract.

(c) When, in the opinion of the Contractor, the COR requests effort outside the scope of the contract, the Contractor will promptly notify the Contracting Officer in writing. No action will be taken by the Contractor under such technical instruction until the Contracting Officer has determined if such effort is within the contract scope, and, if not, has issued a contract change.

Changes in Section J

The following clause which is incorporated by full text has been modified:

J-TXT-01 Section J – LIST OF ATTACHMENTS

TITLE	DATE	NO. OF PAGES
Exhibit A – DD FORM 1423, Contract Data Requirements List	8/29/01	7
Attachment 1- DD FORM 254, Contract Security Classification Specification	9/09/02	23