LOCKHEED MARTIN

LOCKHEED MARTIN CORPORATION

PRIME SUPPLEMENTAL FLOWDOWN DOCUMENT (PSFD)

ADDITIONAL TERMS AND CONDITIONS FOR SUBCONTRACTS/PURCHASE ORDERS UNDER

P3 CUSTOMS AND BORDER PATROLCONTRACT NUMBER: HSBP1009C02278

Generated using Lockheed Martin CorpDocs 2009 Version

24 July 2009

Version 1 (14 September 2009)

The Terms and Conditions listed below are incorporated by reference and made a part of this Contract. Unless otherwise limited in this Contract, each document applies in its entirety.

In the event of a conflict between the version or date of a clause set forth in this document and the version or date of a clause set forth in the identified CorpDocs, the version or date of the clauses set forth in this document shall take precedence.

To the extent that any clause included in this PSFD is inapplicable to the performance of this Contract, the parties shall consider such clauses to be self-deleting and shall not impose any obligations upon the SELLER.

(Use this addendum in addition to the applicable CORP DOC (2 FOR Commercial Items, 3 for Supplies and 4 for cost type contracts, etc.) AND use the applicable CORP DOC D supplement for Homeland Security).

1. VERIFICATION OF SERVICES AND TIME RECORDS

The performance of the Work and the assignment of personnel hereunder shall be subject to random verification by the Government and/or BUYER during the effective period of the contract for the purpose of ensuring the qualifications of assigned personnel, verifying the categories of labor being utilized, ascertaining the accuracy of time and labor charges, preserving the identification of Government equipment and/or parts and material acquired for Government use and otherwise verifying compliance with contractual requirements.

In this regard, SELLER recognizes the Government's and/or BUYER's right to conduct random "checks", provided such are made during working hours and do not unduly delay or inhibit work flow, or SELLER's performance. SELLER agrees to make available, upon request, to Government and/or BUYER personnel, appropriate resumes, individual labor category classifications, pertinent time cards and payroll records, and such other contract associated records as may be required to substantiate contract compliance.

2. GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

Under no circumstances shall SELLER, or anyone acting on behalf of SELLER, refer to the supplies, services,

or equipment furnished pursuant to the provisions of this contract in any news r
advertising without first obtaining explicit written consent to do so from BUYER.

SELLER agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Government or BUYER or is considered by the Government or BUYER to be superior to other products or services.

3. SECURITY PROCEDURES (MAY 2003)

A. Controls

SELLER shall comply with the U.S. Customs & Border Protection (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.

B. Identification Badges

All SELLER employees shall be required to wear identification badges when working in Government facilities.

C. Security Background Data

A SELLER employee shall not begin working under the contract until the entire background investigation (BI) is completed with approval from CBP, Security Programs Division. Exceptions to this requirement will be handled on a case-by-case basis, and access to facilities, systems, data, etc. will be limited until the individual is cleared.

SELLER employee personnel hired to work within the United States or its territories and possessions that require access to CBP facilities, information systems, security items and products, and/or sensitive but unclassified information shall either be U.S. citizens or have lawful permanent resident status.

The following security screening requirements apply to both U. S. citizens and lawful permanent residents who are hired as SELLER personnel. All personnel employed by the SELLER or responsible to the SELLER for the performance of the Work hereunder shall either currently possess or be able to favorably pass a background investigation. The SELLER shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, and date of birth of these people who claim to have successfully passed a background investigation by the CBP, or submit such information and documentation as may be required by the Government to have a BI performed for all personnel. The information must be correct and be reviewed by a Customs Official for completeness. Normally this shall consist of SF-85P, "Questionnaire for Public Trust Positions;" FD-258, "Fingerprint Chart;" and a Financial Statement.

Failure of any SELLER personnel to pass a BI means that SELLER has failed to satisfy the contract's requirement to provide cleared personnel. The continuing failure to meet the requirement to provide cleared personnel is grounds for termination of the contract, unless cleared personnel are timely provided as replacements. SELLER must provide a qualified replacement capable of passing a BI for any person who fails to successfully pass a BI. This policy also applies to any personnel hired as replacements during the term of the contract. The BUYER must approve all personnel replacements.

Estimated completion of the investigation is approximately ninety (90) to one-hundred twenty (120) days from the date the completed forms are received in the Security Programs Division. D. Notification

of Personnel Changes
SELLER shall notify BUYER via phone, FAX, or electronic transmission, no later than one work day after any personnel changes occur. Written confirmation is required for phone notification. This includes, but is not limited to, name changes, resignations, terminations, and reassignments (i.e., to another contract.)

SELLER shall notify BUYER of any change in access requirements for its employees no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other contractors. SELLER shall provide the following information to BUYER: full name, social security number, effective date, and reason for change.

E. Separation Procedures

In accordance with Customs Directive No. 51715-006, "Separation Procedures for Contractor Employees," SELLER is responsible for ensuring that all separating employees complete relevant portions of the Contractor Employee Separation Clearance, CBP Form 242. This requirement covers all SELLER employees who depart while a contract is still active (including resignation, termination, etc.) or upon final contract completion. Failure of SELLER to properly comply with these requirements shall be documented and considered when completing Contractor Performance Reports.

F. General Security Responsibilities During Performance

SELLER shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various CBP regulations pertaining thereto, good business practices, and the specifications, directives, and manuals for conducting work to generate the products as required by this contract. Personnel will be responsible for the physical security of their area and government furnished equipment (GFE) issued to them under the provisions of the contract.

G. Non-Disclosure Agreements

When determined to be appropriate, SELLER employees may be required to execute a non- disclosure agreement as a condition to access of sensitive but unclassified information.

4. DISCLOSURE OF INFORMATION (MAR 2003)

A. General

Any information made available to SELLER by BUYER or the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract.

B. Technical Data Rights

SELLER shall not use, disclose, reproduce, or otherwise divulge or transfuse to any persons any technical information or data licensed for use by the Government that bears any type of restrictive or proprietary legend except as may be necessary in the performance of the contract. Refer to the Rights in Data clause for additional information.

C. Privacy Act

In performance of this contract SELLER assumes the responsibility for protection of the confidentiality of

all Government and BUYER records and/or protected data provided for perf
and shall ensure that (a) all Work performed by any subcontractor is subject to the disclosure restrictions set forth above, and (b) all subcontract work be performed under the supervision of SELLER or its employees.

5. ORGANIZATIONAL CONFLICT OF INTEREST

A. SELLER warrants that, to best of its knowledge and belief, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest, as defined in Federal Acquisition Regulation (FAR) Subpart 9.5, or that SELLER has disclosed all such relevant information in writing to BUYER.

B. SELLER agrees that if an actual or potential organizational conflict of interest is discovered after award, SELLER will make full disclosure in writing to BUYER no later than three working days after discovery. This disclosure shall include a description of actions which SELLER has taken or proposes to take, after consultation with BUYER, to avoid, mitigate, or neutralize the actual or potential conflict.

C. Remedies. BUYER may terminate this contract for convenience, in whole or in part, if it deems such termination necessary to avoid an organizational conflict of interest. If SELLER was aware, or should have been to award of a potential conflict of interest prior to award or discovered an actual or potential conflict after award and did not disclose or misrepresented relevant
information to BUYER, the BUYER may terminate the contract for default, and the Government may debar the SELLER from Government contracting. BUYER may also pursue such other remedies
as may be permitted by law or this contract.

D. SELLER further agrees to insert provisions which shall conform substantially to the language of this clause, including this paragraph D, in any subcontract or consultant agreement hereunder.

6. ACCESS TO GOVERNMENT SITES

If the Work to be accomplished under this contract will be performed at specified Government sites, then SELLER shall be granted access in accordance with Customs and Border Protection and the specific sites' regulations where the Work is to be performed.

While SELLER personnel are at the Government sites, they are required to comply with all rules and regulations of the site. They shall comply with all federal, state, and local government health and safety regulations governing on the job conduct.

7. SECURITY REQUIREMENTS

SELLER shall be responsible for complying with the security requirements as stipulated by the Contract Security Classification Specification (Form DD 254).

A. All SELLER employees that are temporarily deployed, as well as permanently assigned, outside the United States, Puerto Rico, U.S. Possessions and Trust Territories must have, at a minimum, a secret security clearance issued by the Defense Security Service. All SELLER employees requiring access to the various Department of Defense supply systems also must have, at a minimum, a secret security clearance issued by the Defense Security Service.

From time to time, a requirement for additional security clearance may be placed on SELLER. In such cases, BUYER reserves the right to require SELLER to institute additional background investigations of any

SELLER personnel. BUYER shall provide guidance regarding the scope of requirement.

B. SELLER shall be responsible for compliance by its employees with security regulations of Customs and Border Protection and the host Department of Defense (DOD) installation where the Work is performed under this contract, including the safekeeping, wearing and visibility of badges if so required by DOD.

C. SELLER shall be responsible for safeguarding data and protecting against loss or theft of equipment, property, and supplies used in connection with the performance of the Work under this contract.

D. If SELLER's personnel is responsible for installation, troubleshooting (external to the equipment only), and removing cryptographic CBP COMSEC equipment from aircraft,
SELLER will not have access to canisters or segments of CBP COMSEC keying material in any form. Further, SELLER shall only remove CBP COMSEC equipment from aircraft when directed by BUYER. If directed by BUYER, SELLER will be responsible for safeguarding CBP COMSEC
equipment that has been removed and returning it to SELLER or the CBP COMSEC custodian,
as directed. All SELLER personnel who shall perform the above responsibilities shall have, at a minimum, a Secret Security Clearance.

8. NOTICE OF DRUG DETECTION PROCEDURES

Pursuant to military policy applicable to both Government and SELLER personnel, measures
will be taken to prevent the introduction and utilization of illegal drugs and related paraphernalia into Government work areas.

In implementing drug control measures, unannounced periodic inspections of the following nature may be considered by military installation security authorities:

1. Routine inspection of SELLER occupied work spaces.
2. Random inspections of vehicles on entry or exit with drug detection dog teams as available, to eliminate vehicles as a safe haven for storage of or trafficking of illegal drugs.
3. Random inspections of personal possessions on entry or exit of any installations.

When there is probable cause to believe that a SELLER employee on board a military installation has been engaged in use, possession, or trafficking of drugs, the installation authorities may detain said employee until the employee can be removed from the installation, or can be released to the local authorities having jurisdiction.

Trafficking in illegal drugs and drug paraphernalia by SELLER employees while on military installation may lead to possible withdrawal or downgrading of security clearance, and/or referral for prosecution by appropriate law enforcement authorities.

SELLER is responsible for the conduct of employees performing the Work under this contract and is, therefore, responsible to ensure that employees are notified of these provisions prior to assignment.

The removal of SELLER personnel from a Government installation as a result of drug offense(s) shall not be cause for excusable delay, nor shall such action be deemed a basis for an equitable adjustment to price/cost, delivery, or other provisions of this contract.

9. FEDERAL ACQUISITION REGULATIONS

52.215-2 AUDIT AND RECORDS – NEGOTIATION (MAR 2009) (Applies if this contract exceeds $100,000 and if (1) this is a cost-reimbursement, incentive, time and materials or price- redeterminable contract, (2) if SELLER was required to furnish cost or pricing data, or (3) this contract requires SELLER to furnish cost, funding or performance reports.)

52.222-43 FAIR LABOR STANDARDS ACT AND SERVICE CONTRACT ACT – PRICE ADJUSTMENT (MULTIPLE YEAR AND OPTION CONTRACTS)(NOV 2006) (Applies if FAR 52.222-41 Service Contract Act of 1965, as amended, applies to this contract. "Contracting Officer" means "Lockheed Martin and the Contracting Officer" except in paragraph (f) where it means "Lockheed Martin." The notice period in paragraph (f) is changed to twenty (20) days. Adjustments made to this contract shall not be made unless or until the Contracting Officer makes appropriate adjustments to Lockheed Martin's prime contract.)

52.227-23 RIGHTS TO PROPOSAL DATA (TECHNICAL) (JUN 1987) (It is agreed that as a condition of award of this contract, and notwithstanding the conditions of any notice appearing thereon, the Government shall have unlimited rights (as defined in the Rights in Data--General clause contained in this contract) in and to the technical data contained in SELLER'S proposal upon which this contract is based.

10. HOMELAND SECURITY ACQUISITION REGULATIONS

3052.204-71 CONTRACTOR EMPLOYEE ACCESS (JUN 2006) ALTERNATE I (JUN 2006)

(a) Sensitive Information, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act),
but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, compute equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) SELLER employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by BUYER or the Government. Upon BUYER or the Government's request, SELLER's employees shall be fingerprinted, or subject to other investigations as required. All SELLER employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under CBP Departmental procedures.

(d) BUYER may require SELLER to prohibit individuals from working on the contract if the BUYER or Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) The Work under this contract may involve access to sensitive information. Therefore, SELLER shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the BUYER. For those SELLER employees authorized access to sensitive information, SELLER shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) SELLER shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the BUYER will arrange, and complete any nondisclosure agreement furnished by BUYER.

(h) The SELLER shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by BUYER in writing as necessary for performance of the Work under this contract. Any attempts by SELLER personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by BUYER, is strictly prohibited. In the event of violation of this provision, BUYER will take appropriate actions with regard to the contract and the Government will take action as to the individual(s) involved.

(i) SELLER access to DHS networks from a remote location is a temporary privilege for mutual convenience while SELLER performs business for BUYER and the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) SELLER access will be terminated for unauthorized use. SELLER agrees to hold and save BUYER and the Government harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Government IT systems under the contract, unless a waiver has been granted by the Head of the Government component or designee, with the concurrence of both the DHS Chief Security Officer (CSO) and DHS Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a

waiver to be granted:

(1) The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
(2) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
(3) The waiver must be in the best interest of the Government.

(l) SELLER shall identify in its proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the BUYER.