

PASSIVE
RADIO FREQUENCY IDENTIFICATION (pRFID) II

PERFORMANCE WORK STATEMENT

PASSIVE RADIO FREQUENCY IDENTIFICATION TECHNOLOGY II (PRFID-II)
PERFORMANCE WORK STATEMENT (PWS)

Table of Contents

1	SCOPE	5
1.1	PROJECT OBJECTIVES	5
1.2	DESCRIPTION AND SPECIFICATION	5
1.3	GENERAL	6
1.4	PASSIVE RFID APPLICATIONS	6
1.5	GEOGRAPHIC LOCATIONS	6
1.6	RESTRICTION OF HAZARDOUS SUBSTANCES (RoHS)	7
1.7	OFFICIAL HOURS OF OPERATION	7
1.8	ATTACHMENTS AND EXHIBITS	7
2	APPLICABLE DOCUMENTS, DEFINITIONS, AND ACRONYMS.....	7
2.1	FEDERAL INFORMATION PROCESSING STANDARDS	7
2.2	ELECTRONIC PRODUCT CODE (EPC) GLOBAL STANDARDS	7
2.3	FEDERAL COMMUNICATION COMMISSION (FCC) REGULATIONS	7
2.4	UID AND IUID POLICY REGULATIONS	8
2.5	ARMY SECURITY POLICY REGULATIONS	8
2.6	DoD SECURITY POLICY REGULATIONS AND DFARS	8
2.7	OFFICE OF MANAGEMENT AND BUDGET (OMB) CIRCULAR NO. A-130 REVISED	8
2.8	DEFINITION OF TERMS	8
2.9	ACRONYMS	8
3	PASSIVE RFID TECHNOLOGY REQUIREMENTS	10
3.1	GENERAL	10
3.2	DEFENSE INFORMATION STANDARDS REGISTRY (DISR) COMPLIANCE	10
3.3	OPERATING ENVIRONMENTS	11
3.3.1	Electromagnetic Environment	11
3.3.2	Electrostatic Discharge	11
3.3.3	Hazardous Environment.....	11
3.3.4	Ordnance Environment	12
3.3.5	Testing.....	12
3.3.6	Safety.....	12
3.3.7	Device Labels.....	12
3.3.8	Radio Regulatory Compliance	13
3.3.9	Rugged Environment	13
3.4	BAR CODE REQUIREMENTS	13
3.5	ORIGINAL EQUIPMENT MANUFACTURER ENGINEERING CHANGES	13
3.6	CONNECTIVITY TO GOVERNMENT-OWNED COMPUTERS	14
3.7	AC/DC POWER REQUIREMENTS	14
3.7.1	Power Requirements	14
3.7.2	Battery Operated pRFID Readers	14
3.7.3	Rechargeable Batteries	14
3.7.4	Internal Back-up Power.....	14
3.7.5	Battery Protection.....	14
3.7.6	HHR Low-Power Operation.....	15
3.8	ACCESSIBILITY	15
3.9	EQUIPMENT DELIVERY REQUIREMENTS	15
3.10	EXPEDITED DELIVERY REQUIREMENTS	15
3.11	UNIQUE IDENTIFICATION	15
3.12	IPv6 CAPABLE ASSETS	16
3.13	HAZARDS OF ELECTROMAGNETIC RADIATION TO PERSONNEL (HERP)	16
4	PRFID EQUIPMENT REQUIREMENTS	16
4.1	pRFID REQUIREMENTS	16
4.2	PASSIVE RFID FUNCTIONAL / DEVICE REQUIREMENTS	16
4.2.1	pRFID Fixed Reader.....	16
4.2.2	pRFID Vehicle Mount Fixed Reader	17
4.2.3	pRFID Smart Table	17
4.2.4	pRFID HHR	17

4.3	PRFID TAG READABILITY REQUIREMENTS	20
5	SOFTWARE, FIRMWARE, AND SECURITY REQUIREMENTS	21
5.1	SOFTWARE REQUIREMENTS	21
5.1.1	Environment	21
5.1.2	Graphical User Interface	21
5.1.3	Capability	21
5.2	CONFIGURATION / OPERATIONAL SOFTWARE FOR FIXED READER PC	21
5.3	CONFIGURATION / OPERATIONAL SOFTWARE FOR HHR	22
5.4	APPLICATION DEVELOPMENT SOFTWARE	22
5.4.1	PRFID Application Development Software	22
5.4.2	Separately Orderable Components	22
5.4.3	HHR Software Development Kit	22
5.5	PASSIVE RFID ENABLED PRINTER SOFTWARE	22
5.6	FIRMWARE REQUIREMENTS	23
6	SECURITY	23
6.1	HHR AND HHT ACCESS PROTECTION	23
6.2	SECURITY STANDARDS	23
6.3	DOD INFORMATION ASSURANCE REQUIREMENTS	23
6.4	DoD WIRELESS DEVICE SECURITY REQUIREMENTS	24
6.5	ARMY WIRELESS DEVICE SECURITY REQUIREMENTS	24
6.6	COMMON CRITERIA COMPLIANCE REQUIREMENTS	24
6.7	SECURITY CERTIFICATION AND ACCREDITATION SUPPORT	24
6.8	SECURITY MAINTENANCE SERVICES	24
6.9	GOVERNMENT EVALUATION	24
6.10	CYBERSECURITY DOCUMENTATION REQUIREMENTS	25
6.11	UPDATES, INCIDENT REPORTING AND VULNERABILITIES MANAGEMENT	25
6.11.1	IAVAs	25
6.11.2	Security Technical Implementation Guides (STIG)	25
6.12	DESIGN CONSIDERATIONS	25
7	MANAGEMENT	26
7.1	PRFID PROGRAM MANAGEMENT	26
7.1.1	Points of Contact	26
7.1.2	PRFID II Contract Program Manager	26
7.2	USER GUIDE	27
7.2.2	User Guide Review	27
7.2.3	User Guide Approval and Posting	27
7.3	PRFID MANAGEMENT PLAN	29
7.3.1	Integrated Product Teams	29
7.3.2	Project Progress Reviews	30
7.3.3	Status Report	30
7.3.4	Contractor Manpower Reporting (CMR)	31
7.4	CONFIGURATION MANAGEMENT	31
7.4.1	PRFID II Configuration Management Plan	31
7.4.2	Changes and Modifications	32
7.4.3	Changes to Software	32
7.4.4	Notification of Software Changes	32
7.4.5	Correction of Safety Hazards or Equipment Malfunctions	32
7.4.6	Configuration Audits	32
7.4.7	Physical Configuration Audit	33
7.4.8	Functional Configuration Audit	33
7.5	RISK MANAGEMENT	33
7.6	MONTHLY EQUIPMENT AND SERVICE REPORT	33
7.7	WARRANTY STATUS REPORT	34
8	REPAIR REQUIREMENTS	34
8.1	REPAIR CENTERS	34
8.1.1	Points of Contact	34
8.1.2	RC Hours of Operation	34
8.1.3	Equipment Return and Tracking	34
9	CUSTOMER SUPPORT	35
9.1	TECHNICAL ASSISTANCE	35
9.1.1	Toll-Free Customer Support Help Desk	35
9.1.2	Web Site	35

10	WARRANTY	36
10.1	WARRANTY SUPPORT	36
10.2	WARRANTY MAIL-IN PROCEDURES	36
10.3	COMPONENT RETURN AND TRACKING	37
10.4	WARRANTY REPLACEMENT PARTS	37
10.5	WARRANTY ON-CALL PROCEDURES	37
11	MAINTENANCE.....	37
11.1	MAINTENANCE TURN-AROUND TIME	37
11.1.1	pRFID Component Return and Tracking	37
11.1.2	Mail-In Maintenance	38
11.1.3	On-Call Maintenance.....	38
11.1.4	Maintenance Procedures	38
11.1.5	Maintenance Replacement Parts.....	38
11.1.6	Software Maintenance	38
11.2	PREVENTIVE MAINTENANCE	39
11.3	TRANSPORTATION	39
12	TECHNICAL ENGINEERING SERVICES.....	39
12.1	GENERAL	39
12.1.1	Proposal Request for TES	39
12.1.2	Travel.....	40
12.1.3	TES Trip Report	40
12.1.4	TES Response Time	40
12.1.5	Software Development Services	40
12.2	INSTALLATION / DE-INSTALLATION / RELOCATION	40
12.2.1	Site Surveys and Installation Plans.....	40
12.2.2	Installation/De-installation	41
12.2.3	Relocation of Passive RFID Components	41
12.2.4	Installation Plans.....	41
12.3	CONTRACT SUPPORT PERSONNEL	41
13	DOCUMENTATION REQUIREMENTS	42
13.1	GOVERNMENT RIGHTS	42
13.2	COMMERCIAL USER MANUALS	42
13.3	SOFTWARE REFERENCE DOCUMENTATION	42
14	TRAINING REQUIREMENTS	43
14.1	WEB BASED AND CD-ROM TRAINING	43
14.1.1	Target Audiences and Areas.....	43
14.1.2	Training	43
14.1.3	Special Training Materials	43
14.1.4	Training Deliverables.....	44
14.1.5	Training Package Updates.....	44
15	CERTIFICATION.....	44
15.1	PASSIVE RFID CERTIFICATIONS	44
15.1.1	Energy Star.....	44
15.1.2	NI Certification	44
15.1.3	Product Safety Certification.....	44
15.1.4	Electromagnetic Compatibility (EMC) Compliance and Hazards of Electromagnetic Radiation to Ordnance (HERO) Compliance.....	44
15.1.5	Self-Certification.....	45
16	BACKGROUND INVESTIGATIONS FOR CONTRACTOR PERSONNEL	45
16.1	BACKGROUND	45
16.2	NAC FILE RECORDS	45
16.3	CONTINUED PERFORMANCE DURING SUPPORT OF CRISIS SITUATIONS, CONTINGENCY OR EXERCISE	45
17	ORGANIZATION CONFLICT OF INTEREST (OCI).....	46
17.1	NON-DISCLOSURE AGREEMENT	46
17.2	CATEGORIES OF CONFLICTING INTEREST	47
	Exhibit A – Safe Separation Distance.....	48
	Exhibit B – Contract Status Report.....	49

Exhibit C – Antiterrorism/Operations Security Requirements.....50

1 SCOPE

The Mission of Product Director Automated Movement and Identification Solutions (PD AMIS) is to provide a single point of contact for procurement and technical expertise across the suite of Automatic Identification Technology (AIT) enabling technologies that support focused logistics, Total Asset Visibility (TAV), and the integration of global supply chains. The Passive Radio Frequency Identification (pRFID) II Contract provides hardware, software, documentation, and incidental services to authorized users worldwide. Incidental services include training, warranty and maintenance services, and technical engineering services (TES). All Passive RFID hardware conforms to the EPC Global Standards / Specifications for each Class of Tags. In addition, future requirements involving portal readers, extended memory Tags, sensor enabled Tags, and smart fixed readers will be reviewed on a biannual basis to determine applicability with regard to Government use and implementation. Hardware and software delivery and installation, as well as performance of associated training and warranty and maintenance services, will be required at CONUS and OCONUS Government sites. Performance of TES will be required at CONUS and OCONUS Government sites, and the Contractor facility.

1.1 PROJECT OBJECTIVES

The objective of the pRFID II acquisition is to provide a state-of-the-art, common, integrated structure for logistic identification, tracking, locating, and monitoring of commodities and assets. In addition, Item Unique Identification (IUID) marking, data collection, storage information, retrieval methods, information processing, and transmission of Tag data will greatly enhance systems within the Department of Defense (DoD), United States Coast Guard, other Federal Agencies, North Atlantic Treaty Organization (NATO), Coalition Partners and, other Foreign Military Sales (FMS). Passive RFID technology will provide standardization and interoperability amongst Government Users of Passive RFID equipment and incidental services acquired from the pRFID II Contract.

1.2 DESCRIPTION AND SPECIFICATION

This Description and Specification sets forth the requirements for the pRFID II Contract.

The Contract shall provide for commercially available Passive RFID technology communications hardware, software, Technical Engineering Services (TES), documentation, training, and warranty and, maintenance services, to provide a common, integrated structure for logistics tracking, locating, and monitoring of assets for all Users.

The definition of Passive RFID (also referred to as pRFID) components for the purposes of this Contract are those commercial products necessary for pRFID, the tracking of tagged commodities and assets, data collection, keyless data entry, data processing, data storage, and retrieval. The standalone terms “Passive RFID and “pRFID” as used in this Contract initially refer to Passive technology.

The pRFID II Contract provides pRFID hardware and software that will be used in fixed and mobile locations. The pRFID II requirements include, but are not limited to, microprocessor-based RFID hardware, software, data communications, and turnkey integration services to include: pRFID Tags, pRFID Fixed Readers; pRFID Enabled Printers; pRFID Hand Held Readers (HHR); pRFID Vehicle Mount Readers; pRFID Smart Tables; Rechargeable Batteries and Battery Chargers; Software (Configuration/Operational Software for PC, Configuration/Operational Software for HHR, Application Development Software and Special Software Development Tool Kits/Utility Libraries, Integration Software, pRFID Enabled Printer Software); upgrades and updates to all delivered Software; Separately Orderable Components; TES (Installation, De-installation, and Relocation of pRFID components); Software Development Services; Middleware Development Services for Task Order (TO)s; Commercially

available Middleware for TOs; System Integration; IUID marking and Implementation Support; Warranty; Maintenance; Program Management; and Training.

Turnkey solutions integrating technology purchased under the pRFID II Contract with existing Government provided AIT and Active RFID shall be provided under TES TOs to provide a transparent solution to the User. The pRFID Tags provided under this Contract shall have 100% readability in an optimal environment, as defined by the Contractor, when applied to but not limited to the following materials: metals, fiberboard, plastic, wood, and glass. pRFID Tags (available in roll form) provided on this Contract shall be compatible with the printer provided under this Contract. pRFID printers shall write to and correctly verify programmed Tags after printing / encoding. pRFID technologies are applied to areas such as inventory and warehousing environments; supply chain tracking, control of maintenance, repair, and tracking facilities; control of entry and exit points of military facilities, and roadside installations; control of transactions at custody exchange points (e.g., weapons issue facilities); the military transportation community (e.g., seaports and aerial ports); the handling of hazardous explosives; and for other regulated materials.

The Government reserves the right to add a transit case(s) to the Contract to support missions that require rapid deployment worldwide of groups of pRFID equipment. In the event the Government has a requirement to add a transit case(s) to the Contract, the Contracting Officer (KO) will request a Contract Change Proposal (CCP), and the Contractor shall submit a CCP in accordance with the paragraphs "Current Technology Substitutions and Additions" and "Contract Change Proposal (CCP) Response Time" stated in Section H.

1.3 GENERAL

The Government shall utilize pRFID technologies in applications that demand performance on a higher level than that available with bar code and other automated data storage and retrieval technologies. Passive RFID Tags will be affixed to pallets, cases, and assets or other objects of interest to capture and transmit varying amounts of data, which can be stored (either permanently or temporarily) and processed. The Government requires pRFID Readers that shall be programmable to read pRFID Tags. The Reader shall read and write information to pRFID Tags. This feature shall enable a User to locate, track, and monitor the status of a Tag and its associated commodity and asset, or to alter the data stored on a Tag.

1.4 PASSIVE RFID APPLICATIONS

Some anticipated applications of pRFID technology include, but are not limited to the following:

- a. Inventory and warehousing environments;
- b. Supply chain tracking;
- c. Large open-area storage facilities (austere marshaling areas, and staging and assembly areas), with or without electrical power or an established communications infrastructure;
- d. The control of maintenance, repair, and tracking facilities;
- e. The control of entry and exit points of military facilities, and roadside installations;
- f. Restricted office and laboratory environments;
- g. The control of transactions at custody exchange points (eg., weapons issue facilities);
- h. The military transportation community (eg., seaports and aerial ports), and petroleum distribution points (including fueling operations at airports, in-flight and at sea);
- i. The handling of hazardous, explosive, or otherwise regulated materials; and
- j. The control of military convoys.

1.5 GEOGRAPHIC LOCATIONS

The Government requires equipment that can be used worldwide in accordance with the EPC Global Standard, Version 2.0 (excluding Japan).

1.6 RESTRICTION OF HAZARDOUS SUBSTANCES (ROHS)

All hardware provided under the Contract shall comply with the Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0095:EN:HTML>.

1.7 OFFICIAL HOURS OF OPERATION

The Contractor shall provide support during local Official Hours of Operation (defined in paragraph "Definition of Terms" in this Part), based on the geographic location of the Government site at which the support will be provided except for Hours of Operation requirements that are specified in paragraphs "Toll-Free Customer Support Help Desk" and "On-Call Maintenance" in this Part.

1.8 ATTACHMENTS AND EXHIBITS

The following exhibits are contained in Section J:

- a. Exhibit A - Safe Separation Distance between a RF Source and Unshielded Munitions Containing 10 mA No-fire Current Electro-explosive Devices (EEDs).
- b. Exhibit B – pRFID II Contract Status Report

2 APPLICABLE DOCUMENTS, DEFINITIONS, AND ACRONYMS

2.1 FEDERAL INFORMATION PROCESSING STANDARDS

Copies of the Federal Information Processing Standards (FIPS) may be obtained from the following:

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
Telephone: 1-800-553-6847
<http://www.ntis.gov/>

2.2 ELECTRONIC PRODUCT CODE (EPC) GLOBAL STANDARDS

Copies of the EPC Global Standards may be obtained from the following:

EPC Global US
Princeton Pike Corporate Center
1009 Lenox Drive, Suite 202
Lawrenceville, NJ 08648
Phone: 609.620.4671
Fax: 609.620.0255
Website: <http://www.epcglobalinc.org/standards>

2.3 FEDERAL COMMUNICATION COMMISSION (FCC) REGULATIONS

FCC Regulations can be obtained from the Government Printing Office web site listed below:

<http://www.access.gpo.gov/cgi-bin/cfrassemble.cgi?title=200547>

International Transcription Services
2100 M. Street, N.W., Suite 140
Washington, DC 20037
Telephone Ordering: 202-512-1800

2.4 UID AND IUID POLICY REGULATIONS

Updates to Policy and associated Guides for Unique Identification (UID) and Item Unique Identification (IUID) of Tangible Items, can be obtained from the following:

<http://www.uidforum.com/>

<http://www.acq.osd.mil/dpap/pdi/uid/index.html>

2.5 ARMY SECURITY POLICY REGULATIONS

http://www.army.mil/usapa/epubs/25_Series_Collection_1.html

2.6 DOD SECURITY POLICY REGULATIONS AND DFARS

Security Policy Regulations: <http://www.dtic.mil/>

DFARS: <http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html>

2.7 OFFICE OF MANAGEMENT AND BUDGET (OMB) CIRCULAR NO. A-130 REVISED

<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>

2.8 DEFINITION OF TERMS

The following are definitions of terms used in this Specification. All other definitions and meanings used in this Specification will be those that are commonly used in the Radio Frequency Identification Technology (RFIT) industry.

- a. Continental United States (CONUS): All locations and sites within the 48 contiguous States.
- b. Industrially Hardened Components: Components that can operate in a warehouse or manufacturing setting and are capable of surviving the rough treatment and handling often found in shipping areas, loading docks, catwalks, ladders, or on the floor of a manufacturing facility.
- c. Non-incendive (NI): See paragraph 3.3.3 entitled "Hazardous Environment."
- d. Outside Continental United States (OCONUS): All locations outside the 48 contiguous States of the U.S. OCONUS locations include, but are not limited to, Alaska, Hawaii, U.S. Territories and Possessions, Europe, Asia, and Australia.
- e. Official Hours of Operation: Official hours of operation are from 8:00 a.m. to 5:00 p.m. local time, Monday through Friday, excluding Federal holidays, for each Government facility possessing Passive RFID components.
- f. Return Material Authorization (RMA): This is a number that shall be assigned by the Contractor for tracking Passive RFID EPC Global components returned for warranty or maintenance service. This number shall be furnished to the RFID user to assist in ascertaining the status of those components.

2.9 ACRONYMS

The following are acronyms used in this Specification:

AC	Alternating Current
AIS	Automated Information System
ANSI	American National Standards Institute
AR	Army Regulation
CLIN	Contract Line Item Number
CAC	Common Access Card
CCPP	Common Criteria Protection Profile

CCTL	Common Criteria Test Laboratory
CDMA	Code Division Multiple Access
CISPR	International Special Committee on Radio Interference
CONUS	Continental United States
COR	Contracting Officer's Representative
DIACAP	Dept of Defense Information Assurance Certification and Accreditation Process
DISR	Defense Information Standards Registry
DC	Direct Current
DO	Delivery Order
DoD	Department of Defense
DoDD	Department of Defense Directives
DoDI	Department of Defense Instruction
DSS	Defense Security Service
EAN	European Article Numbering System
EC	Engineering Change
EED	Electro-Explosive Devices
EIT	Electronic and Information Technology
EMC	Electromagnetic Compatibility
EPA	Environmental Protection Agency
EPC	Electronic Product Code
FCA	Functional Configuration Audit
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FMS	Foreign Military Sales
FSC	Federal Service Code
GIG	Global Information Grid
GUI	Graphical User Interface
HERO	Hazards of Electromagnetic Radiation to Ordnance
HERP	Hazards of Electromagnetic Radiation to Personnel
HHR	Hand- Reader
IA	Information Assurance
IPV	Internet Protocol Version
IEEE	Institute of Electrical and Electronics Engineers
IPT	Integrated Product Team
IUID	Item Unique Identification
DISR	Defense Information Standards Registry
KO	Contracting Officer
MESR	Monthly Equipment Service Report
MSDS	Material Safety Data Sheets
NAC	National Agency Check
NEC	National Electrical Code
NI	Non-incendive
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
NSA	National Security Agency
NSN	National Stock Number
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States
OEM	Original Equipment Manufacturer
OG	Ordering Guide
PC	Personal Computer
PCA	Physical Configuration Audit
PM	Product Manager
POC	Point of Contact
PPR	Project Progress Review

PWS	Performance Work Statement
RC	Repair Center
RF	Radio Frequency
RFID	Radio Frequency Identification
RMA	Return Material Authorization
SDK	Software Development Kit
SDS	Software Development Services
SLIN	Sub-Line Item Number
SOW	Statement of Work
TCP/IP	Transmission Control Protocol/Internet Protocol
TES	Technical Engineering Services
TO	Task Order
WLAN	Wireless Local Area Network
UCAPL	Unified Capabilities Approved Products List
UG	User Guide
UIC	Unit Identification Code
UID	Unique Identification
UL	Underwriters Laboratory
UPC	Universal Product Code
USB	Universal Serial Bus

3 PASSIVE RFID TECHNOLOGY REQUIREMENTS

3.1 GENERAL

The Contractor shall provide all necessary hardware, software, data communications, cables, connectors, peripherals, training, installation support services, TES, and documentation (e.g., User Manuals) to operate and maintain the pRFID technologies as stated in this Specification. Due to the diversity of applications, the Contractor shall provide the TES necessary to configure, install, interface, and integrate, the appropriate hardware and software to satisfy specified applications, which will be identified in the TES TO. The Government requires equipment that supports the requirements of the Joint Technical Architecture, if applicable. The Government requires Contractor support during Official Hours of Operations except for Hours of Operation requirements that are specified in paragraphs "Toll-Free Customer Support Help Desk" and "On-Call Maintenance" in this Part. The Government requires commercial software packages and software for application development. Program Management is required to support the Government's efficient execution of this Contract. Warranty services are required to ensure the operational availability of pRFID equipment. TES / Turnkey solutions are required to help the Government incorporate pRFID equipment into various Automated Information Systems (AIS). Training and documentation are required to inform and educate the Government User.

3.2 DEFENSE INFORMATION STANDARDS REGISTRY (DISR) COMPLIANCE

The DISR is the minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements that together form an information system. Its purpose is to ensure that DoD systems are interoperable, scalable, and portable. The pRFID II equipment specified in this Contract is not considered by DoD to be a system. Rather, pRFID II equipment is used to provide data entry front-ends for DoD systems. This Specification includes small computer platforms and components that may be proprietary, or that have neither the capacity nor the scope to satisfy DISR requirements. For example, the operating systems for Hand Held Terminals (HHT) do not meet Common Operating Environment requirements. DISR requirements for modeling and designing a system are also not required by this Contract. Systems developers incorporating pRFID II equipment purchased from this Contract will address product modeling and design requirements in their system models and designs. The DISR requirement for purposes of this Contract is for pRFID II equipment to interface with supported systems. Interface requirements for pRFID II equipment are part of the specifications for these components. For each component provided by the Contractor, the Contractor shall identify each external interface of the component for which a standard

interface specified in the DISR applies, and shall certify that each interface is compliant with a DISR standard.

3.3 OPERATING ENVIRONMENTS

The pRFID II equipment may be subject to operating in diverse / rugged environments, and under a full spectrum of climatic conditions (eg., desert and Arctic areas). The pRFID II equipment may be subject to rough handling, shock, and vibration during transportation, setup, and dismantling. The pRFID II equipment shall be capable of use in industrial, hazardous, and ordnance environments, on board surface and subsurface naval vessels, aircraft, tanks, in conditions that range from protected and controlled (office settings) to extremely harsh and severe environments and in areas with high levels of electromagnetic noise and interference. All components acquired from this Contract shall meet applicable Environmental Protection Act (EPA) requirements. The Government requires pRFID equipment that shall operate in the following environments: electromagnetic, hazardous, ordnance and radio frequency environments. The Government requires pRFID equipment that shall operate, at a minimum, in the following temperature ranges:

pRFID Fixed Reader
Operating Temperature - -4 to 120 degrees F
Storage Temperature - -4 to 140 degrees F

pRFID Hand Held Reader (HHR)
Operating Temperature - 32 to 120 degrees F
Storage Temperature - -4 to 140 degrees F

pRFID Enabled Bar Code Label Printer
Operating Temperature – 45 to 95 degrees F
Storage Temperature – 25 to 100 degrees F

3.3.1 Electromagnetic Environment

Commercial pRFID equipment may be used in vicinity with spectrum-dependent devices that receive low-level signals and/or transmit high-level signals (See MIL-STD-464C: Interface Standard for Systems Electromagnetic Environmental Effects). In order to certify the use of commercial pRFID equipment in these environments, the Government may subject representative categories of equipment to radiated emission and susceptibility tests (See MIL-STD 461F: Requirements for the Control of Electromagnetic Interference Emissions and Susceptibility). The Contractor shall provide timely support for Government-testing efforts by providing technical data sheets and responding to Contracting Officer's Representative (COR) requests for additional data.

3.3.2 Electrostatic Discharge

Commercial pRFID packaging of the Tags shall control and dissipate the effects of electrostatic discharge, minimally 5kV, with regard to the degradation or damage to the electronics, which make up the components of the Tag.

3.3.3 Hazardous Environment

The Contractor shall provide, no later than 90 days after the Notice to Proceed, equipment that is identified and certified as NI for operation in environments where flammable and explosive gases and vapors may be present, where specifically required in this Specification. The following minimum NI requirements shall be met:

1. Class 1 and 2 (Gases and Vapors)
Division 2 (Not present in normal operation)
Groups

- A (Acetylene)
 - B (Hydrogen)
 - C (Ethyl Ether, Ethylene)
 - D (Acetone, Ammonia, Benzene, Butane, Cyclopropane, Ethanol, Gasoline, Hexane, Methanol, Methane, Natural Gas, Naphtha, Propane)
2. Class 2 (Combustible Dust)
- Division 2 (Not present in normal operation)
 - Groups
 - F (Combustible carbonaceous dusts)
 - G (All other combustible dusts, such as grain dust)
3. Class 3 (Easily Ignitable Fibers)
- Division 2 (Not present in normal operation)

NI is a rating classification of equipment specifically defined in the National Electrical Code (NEC). In order to receive a NI rating, the Contractor shall have demonstrated under normal operation equipment cannot produce a spark or other undesirable effects that might cause combustion in any potentially hazardous environment. The presence of gases, vapors, flammable liquids, combustible dust, or ignitable fiber or filings are examples of potentially hazardous environments. Equipment shall be certified by an approved testing laboratory meeting Occupation Safety Hazards Act standards. Circuits shall not be capable of producing a spark under normal operation. The pRFID II equipment may be used under conventional, chemical, or biological warfare conditions. The Contractor shall label Passive RFID II components that are approved for use in a hazardous environment in accordance with governing body markings.

3.3.4 Ordnance Environment

The pRFID equipment may be used near ordnance susceptible to radiated energy. In order to certify the use of pRFID equipment in these environments, the Government may subject representative categories of equipment to stringent Hazards of Electromagnetic Radiation to Ordnance (HERO) environment testing (See MIL-STD 464C). The Contractor shall support HERO testing via a TES TO.

3.3.5 Testing

The Contractor shall support Government-testing efforts by providing technical data sheets and responding to the COR's requests for additional data.

3.3.6 Safety

A determination of the required safe separation distance can be made by referring to the graph entitled "Safe Separation Distance Between an RF Source and Unshielded Munitions Containing 10 mA No-fire Current Electro-Explosive Devices (EEDs)" in Exhibit-A. This graph relates safe separation distances to irradiate output power as a function of operating frequency. Although many ordnance items have no EEDs, and other items have EEDs that are less sensitive to RF energy, this requirement represents a worst-case scenario that ensures safe operation around what frequently is unknown ordnance (unknown to transporters and others).

3.3.7 Device Labels

All items requiring HERO testing shall have a warning label affixed to each item that clearly indicates the safe separation distance that must be maintained between ordnance and the irradiating source after HERO evaluation is completed after contract award. The safe separation distance will be determined after HERO testing is completed (post-award). All separation distances shall be specified and added to labeling at that

time. All equipment shall be clearly marked with applicable pRFID and Wireless Local Area Network (WLAN) operating frequency ranges. All equipment certified as NI shall be marked in accordance with the NEC. Any Common Access Card (CAC) Reader that is not certified for NI operation shall have a label affixed which states "Not for use in an NI environment".

3.3.8 Radio Regulatory Compliance

The Government requires pRFID technologies that operate in worldwide frequency spectrums. DoD will obtain "Equipment Frequency Allocation Guidance" approvals for procuring equipment that is designed to either emit or receive electromagnetic (radio frequency) energy. DoD will also obtain frequency assignments to operate the items at each specific location in CONUS. The Government will operate equipment acquired under this Contract consistent with Federal regulations governing the use of the electromagnetic spectrum and the policies and procedures of DoD Directives (DoDD) and Instructions (DoDI): DoDI 3222.3 Operation of the DoD Electromagnetic Environmental Effects Program; DoDD 4650.1 Policy for Management and Use of the Electromagnetic Spectrum; DoDD 5000.1 The Defense Acquisition Program; and DoDI 5000.2 Operation of the Defense Acquisition Program. To facilitate obtaining frequency allocations and assignments in CONUS, the Government requires equipment that is non-licensed to comply with National Technical Information Association Manual Annex K and with FCC Part 15, regulations for Government operations. In order to verify the use of pRFID II equipment the Government may subject selected pieces of equipment to electromagnetic compatibility tests (see MIL-STD-461F). The Contractor shall provide all technical data required to complete a DD Form 1494, Application For Equipment Frequency Application, after Contract award to support the DoD frequency allocation-to-equipment process, including information concerning specifications and testing of the transmitter, receiver and antenna characteristics.

3.3.9 Rugged Environment

Certain pRFID II equipment will be used by the Government in "rugged environments" (i.e., industrial and field settings under temperate, arctic, maritime and desert conditions). The words "rugged" or "ruggedized," when used herein mean that the Government requires that such pRFID equipment be designed, built, and tested to ensure reliable and continuous performance in all rugged environments. In this environment, pRFID equipment may be subjected to rough handling, continuous operational use, vibration, dropping onto hard surfaces, and shock caused by transportation over rough terrain.

3.4 BAR CODE REQUIREMENTS

When bar code capability is required by this specification, equipment and software shall decode and printers shall print symbologies that comply with industry standards and specifications for Code 39, Code 128, CODABAR, Interleaved 2 of five, European Article Numbering System (EAN), Universal Product Code (UPC), PDF 417, and Data Matrix ECC 200. Where bar code capability is required by this specification, the Contractor-provided equipment shall provide for the printing and decoding of the data printed on the Passive RFID EPC Global Enabled Bar Code Labels per these standards. Equipment shall be capable of printing or decoding these symbologies with a nominal 'x' dimension of 10 mils for linear and PDF (10 mil cell module width for Data Matrix).

3.5 ORIGINAL EQUIPMENT MANUFACTURER ENGINEERING CHANGES

All Original Equipment Manufacturer (OEM)-sponsored Engineering Changes (ECs) adopted prior to the date of Contract award shall be incorporated into the hardware and software delivered under this Contract.

3.6 CONNECTIVITY TO GOVERNMENT-OWNED COMPUTERS

The Government currently uses a wide variety of processor-based computers that will connect with the Contractor-provided pRFID equipment. Connections shall be in accordance with standard protocols (ex., RS-232, RS-485, Universal Serial Bus (USB), TCP/IP, Institute of Electrical and Electronics Engineers (IEEE) 802.11).

3.7 AC/DC POWER REQUIREMENTS

3.7.1 Power Requirements

The Contractor shall provide equipment designed and certified to meet quality and safety standards of Underwriters Laboratory (UL) or an equivalent laboratory. The Contractor shall provide pRFID equipment equipped with power supplies, fuses, adapters, and cables to use with locally available commercial power. The pRFID equipment shall be compatible with the power supply, and power outlets or connectors, for the geographic area in which the component is to be operated as specified in the TO/ Delivery Order (DO), or purchase card order. Plug Types for various geographic locations are listed on the web site: <http://ww2.interpower.com/designers/designing-for-export/guides-and-charts/guide-to-worldwide-plugs-and-sockets-patterns-power-mains-single-phase/>.

3.7.2 Battery Operated pRFID Readers

Each battery operated Reader shall be delivered with two sets of rechargeable batteries (one complete set of operational batteries and one complete set of spare batteries) and an AC Adapter (if required for AC operation).

3.7.3 Rechargeable Batteries

Rechargeable Batteries shall provide sufficient capacity to allow a minimum of four hours of continuous Reader operation. Rechargeable Batteries shall not require discharge in order to attain full functionality and total rated battery capacity. The Contractor shall provide rechargeable batteries that are capable of charge operations without removal from pRFID II equipment. All rechargeable batteries shall be User-replaceable by hand or with the use of commonly available tools. The Contractor shall provide battery chargers as Separately Orderable Components, and shall replace re-chargeable batteries during the warranty period for batteries that are found defective (e.g., will not hold four-hour charge). The Contractor may provide battery chargers designed either to charge a single operating set of batteries, or to charge multiple battery sets concurrently.

3.7.4 Internal Back-up Power

The Contractor shall provide:

- a. A method to maintain the configuration settings within all applicable pRFID II equipment (any HHR, Reader, or other products that include firmware);
- b. A method for the configuration settings to be maintained for a minimum of 400 hours when the rechargeable battery or the AC Adapter power (if required for AC operation) is not available;
- c. A method for the rechargeable battery or AC Adapter power (if required for AC operation) source to recharge the internal back-up power source, if any.

3.7.5 Battery Protection

The Contractor shall provide a methodology to prevent premature battery depletion while in shipment or in storage before initial use for any device containing non-rechargeable batteries.

3.7.6 HHR Low-Power Operation

Battery-operated Hand-Held pRFID Readers shall provide the User at a minimum with a low battery power indicator. The low-battery power indicator shall provide the User with at least five minutes of advanced warning of an automatic shutdown. Battery-operated HHR shall automatically shut down before battery power is completely exhausted in order to preserve stored data and conserve power. Battery-operated HHR shall have an automatic, User-definable, time-out capability to conserve battery power during periods of inactivity. The Government requires a feature that allows the User to terminate the time-out period and restore full operation with a single command to the Reader.

3.8 ACCESSIBILITY

The Contractor shall provide a comprehensive list of all provided specific electronic and information technology (EIT) products (supplies and services) that fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's EIT Accessibility Standards at 36 CFR Part 1194. The Contractor shall clearly indicate where this list with full details of compliance can be found (e.g., Contractor, subcontractor, vendor's, or other exact web page location). The Contractor shall ensure that the list is easily accessible by a typical User beginning five calendar days after receipt of the pRFID II Contract award. The Contractor shall maintain this detailed listing of compliant products for the full Contract term, including all forms of Contract extensions, and shall ensure that the detailed listing is updated no later than three calendar days of any changes to the Contractor's, subcontractor's, or vendor's product line. The Contractor shall ensure that all EIT products that are not fully compliant are the most compliant products and services available to satisfy this pRFID II Contract. The Contractor shall, for every EIT product provided under this pRFID II Contract that does not comply with 36 CFR Part 1194, make every effort to replace or upgrade it with a compliant product or service, if commercially available at no additional cost to the Government.

3.9 EQUIPMENT DELIVERY REQUIREMENTS

The Contractor shall provide all necessary software, cables, power adapters, connectors, drivers, essential accessories, and ancillary items in order to make each deliverable hardware item fully operational, which meets the intent of this Contract. All wireless products (such as, but not limited to HHRs, Access Points, Network switches /controllers) shall include an integrated, certified, interoperable FIPS 140-2 security solution and shall be WPA2 compliant (certified to the IEEE 802.11i interoperability standard).

3.10 EXPEDITED DELIVERY REQUIREMENTS

The Contractor shall provide Expedited Delivery for CONUS and OCONUS locations when specified in equipment orders (DOs and Governmentwide Purchase Card Orders). Delivery shall comply with the requirements of the paragraph entitled "Expedited Delivery" in Section H.

3.11 UNIQUE IDENTIFICATION

Applicable items, as identified in DFARS 252.211-7003, Item Identification and Valuation (Aug 2008), in Contract Section I, shall be permanently marked in accordance with the "Revision of Update to Policy for UID and IUID of Tangible Items - New Equipment, Major Modifications, and Re-procurement of Equipment and Spares," December 22, 2003. Marking shall include the UID on the item or identification plate in Data Matrix Bar Code symbology with Human Readable Interpretation (if adequate space is available). Data format shall be in accordance with the "Department of Defense Guide to Uniquely Identifying Items," Version 2.0, October 1, 2008. See Paragraph "UID and IUID Policy Regulations" in section 2.4 for the website for UID and IUID Policy Regulations.

3.12 IPV6 CAPABLE ASSETS

The Contractor shall warrant that each item delivered under the pRFID II Contract shall accurately transmit, receive, process, and function correctly using the Internet Protocol Version 6 (IPv6). Specifically, the Contractor warrants that: 1) each item delivered complies with the current DISR developed IPv6 standards profile; 2) each item delivered maintains interoperability with IPv4 (specifically, shall operate on/coexist on a network supporting IPv4 only, IPv6 only, or a hybrid of IPv4 and IPv6); and 3) each item delivered is supported by the Contractor's IPv6 technical support. Additionally, as IPv6 evolves, the Contractor shall upgrade or provide an appropriate migration path for each item delivered. The duration of this warranty and the remedies available to the Government for breach of this warranty shall be as defined in, and subject to, the terms and limitations of the Contractor's standard commercial warranty or warranties contained in this Contract, provided that notwithstanding any provision(s) to the contrary in such commercial warranty or warranties, the remedies available to the Government under this warranty shall include repair or replacement of any product whose non-compliance is discovered and made known to the Contractor no later than one year after acceptance. Nothing in this warranty shall be construed to limit any rights or remedies the Government shall otherwise have under this pRFID II Contract with respect to defects other than IPv6 performance.

3.13 HAZARDS OF ELECTROMAGNETIC RADIATION TO PERSONNEL (HERP)

The Contractor shall ensure that all equipment provided under the Contract shall comply with all applicable human exposure to Radio Frequency (RF) safety standards per the following regulations:

- a. DODI 6055.11 - Protection of DoD Personnel from Exposure to Radiofrequency Radiation and Military Exempt Lasers
- b. IEEE Standard C95.1, 1999 Edition - IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz
- c. CFR 47 Chapter I, Part 1, Subpart I, Section 1.1310 - Radiofrequency radiation exposure limits
- d. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management - 8.2.28 Radiation Hazards, and Annex K - Technical Standards for Federal "Non-Licensed" Devices

4 pRFID EQUIPMENT REQUIREMENTS

4.1 pRFID REQUIREMENTS

- a. The Government requires all pRFID Tags be read and written, using a variety of Readers as described in this Part.
- b. All pRFID Readers and Printers provided under this Contract shall be furnished with labels clearly indicating: (1) that the item is approved for use in either of the two frequency ranges specified, and (2) appropriately marked in accordance with requirements of paragraph 3.3.7 above. The Contractor shall maintain a current and updated list of countries and frequencies, and provide equipment (by country) approved for use in the country designated in the government order. All products shall be marked with the frequency, or in accordance with the host-country regulations.

4.2 PASSIVE RFID FUNCTIONAL / DEVICE REQUIREMENTS

4.2.1 pRFID Fixed Reader

The Contractor shall provide 902-928MHz and 862 MHz-870 MHz pRFID fixed Readers that shall read pRFID tags without any firmware and software changes. The reading range of Tags shall be attenuable from its maximum operating distance to near contact through the Reader's firmware or other easily addressable method. The Readers shall accommodate a minimum of two antennas. The Reader shall read a minimum of 100 tags per second. The write range of Tags shall be attenuable from its maximum operating distance to near contact through the Reader's firmware or other easily addressable method. The pRFID Fixed Readers shall also be easily upgradeable to accommodate any future firmware changes. In

addition, the pRFID Fixed Readers shall be easily installed by one individual in a location using the Contractor-provided, separately orderable, Mounting Kit. The Contractor shall provide a Mounting Kit as a Separately Orderable Component.

4.2.2 pRFID Vehicle Mount Fixed Reader

The Contractor shall provide 902-928MHz and 862 MHz~870 MHz pRFID Vehicle Mount Readers that shall read pRFID tags without any firmware and software changes. The reading range of Tags shall be attenuable from its maximum operating distance to near contact through the Reader's firmware or other easily addressable method. The Vehicle Mount Reader shall include a minimum of two antennas. The Reader shall read a minimum of 100 tags per second. The Vehicle Mount Reader is intended to read all tags being transported by the vehicle, from single items to a complete pallet load. The Vehicle Mount Reader is intended only to read Tags transported by the vehicle. The pRFID Vehicle Mount Readers shall also be easily upgradeable to accommodate any future firmware changes. In addition, the Vehicle Mount Readers shall include all wiring, power adapters (for forklift power), hardware required for mounting, installation, and operation on a standard industrial warehouse vehicle.

4.2.3 pRFID Smart Table

The Contractor shall provide 902-928MHz and 862 MHz~870 MHz pRFID Smart Tables. The Smart Table shall include fixed Readers that shall read / write Class 1, Gen 2, tags without any firmware and software changes. The reading range of Tags shall be attenuable from its maximum operating distance to near contact through the Reader's firmware or other easily addressable method. The Smart Table shall include an appropriate antenna configuration to function to its' fullest extent. The Reader shall read Tags which are placed on or above the table or placed in non-metallic containers or shipping cartons on the table. The Reader shall not read tags that are removed from the proximity of table. The Reader shall read a minimum of 100 tags per second. The write range of Tags shall be attenuable from its maximum operating distance to near contact through the Reader's firmware or other easily addressable method. The pRFID Smart Table shall also be easily upgradeable to accommodate any future firmware changes. The Smart Table shall be suitable for packing and shipping operations in an industrial warehouse setting, with a minimum working surface of 30" by 48" and a maximum working surface of 48" x 48".

4.2.4 pRFID HHR

The Contractor shall provide HHRs that can read and write to pRFID Tags. The Readers shall be capable of reading a minimum of 100 tags per second. The reading range of Tags shall be attenuable from its maximum operating distance to within 1/32 of an inch through the Readers' firmware or other easily addressable method. The write range of Tags shall be attenuable from its maximum operating distance to within 1/32 of an inch through the Readers' firmware or other easily addressable method. The pRFID HHRs shall also be easily upgradeable to support future product revisions. The pRFID HHRs shall be an ergonomically designed unit that shall be functionally equivalent to the Fixed Reader. The pRFID HHR shall be User-programmable, and shall provide the User with assistance or prompts to perform required functions.

The pRFID HHRs shall be portable and powered by Rechargeable Batteries. Each pRFID HHR, antenna, power supply, and any component required for operation shall be integrated to operate as a one-piece Hand-Held unit with a trigger handle. The pRFID HHR shall have installed Microsoft Windows Mobile 6.x or a later version. The HHRs shall have Common Criteria Certification for Windows Mobile incorporated. In the future, should relevant AIT equipment specific Common Criteria Protection Profiles (CCPP) be adopted, the HHRs will be required to be compliant a the Medium Robustness level within one year of CCPP adoption announcement.

The pRFID HHRs shall have a manual data input interface as well as User-programmable functions. The manual data input interface shall be capable of utilizing a full alphanumeric data entry system (26 alphabetic and 10 numeric characters). The pRFID HHRs shall have a User-selectable, night-readable display, capable of displaying at least 80 characters without scrolling. The Government requires that the

pRFID HHRs be capable of scanning and decoding the linear and 2D symbologies listed in the paragraph entitled "Bar Code Requirements." The pRFID readers shall operate in rugged environments. The Government desires pRFID HHRs that can operate in a wider temperature range than the environmental temperatures stated in the paragraph entitled "Operating Environments" in section 3.3. Radio Frequency Data Communication capability shall be included in the HHR and shall conform to the requirements of IEEE 802.11a or b or g, with user ability to configure for a, or b, or g, or any combination thereof. All IEEE 802.11a or b or g products include an integrated, certified, interoperable FIPS 140-2 security solution and shall be WPA2 compliant (certified to the IEEE 802.11i interoperability standard).

Each HHR shall include a communications/charging dock with appropriate power supply and power cable, a complete set of operational batteries, and a complete set of spare batteries. The communications/charging dock shall support charging the HHR operational battery without removal from the HHR and simultaneous charging of the spare battery. The communications dock shall provide for both USB and Ethernet connectivity of the HHR.

Each HHR shall include an integrated memory storage card with a minimum of 2GB.

HHRs shall include a utility program to monitor and display battery status.

This device, as all hardware items, is subject to the Equipment Delivery Requirements described in paragraph 3.9 and the Security Standards described in paragraph 6.2, of this document. Hardware is required to be fully operational.

4.2.4.1 Separately Orderable Components

CAC Reader including CAC Reader software. If the CAC Reader is not certified for NI operation, there shall be a label affixed which states "Not for use in an NI environment". If the CAC Reader utilizes Bluetooth radio communications, the Bluetooth communications must be FIPS 140 encrypted.

Carrying Device for carrying the HHR, which shall be hands-free device (e.g., holster or belt clip).

Rechargeable Battery

AC Adapter

4.2.4.2 HHRs shall be offered in the following configurations:

4.2.4.2.1 A Model, Standard 902-928MHz and 862 MHz~870 MHz
Shall meet all requirements as stated in paragraph 4.2.4 above.

4.2.4.3 B Model, NI 902-928MHz and 862 MHz~870 MHz

In addition to the requirements stated in paragraph 4.2.4 above, Model B HHRs shall be certified NI as described in the paragraph titled "Hazardous Environments", paragraph 3.3.3 in this document.

4.2.4.4 C Model, Special Configuration, 902-928MHz

In addition to the requirements for HHRs stated in paragraph 4.2.4 above, Model C HHRs shall include the following features:

a. Special Features

1. C Model HHRs shall have alphanumeric keypad, and be certified NI as described in the paragraph titled "Hazardous Environments" in this document. They shall include a Code Division Multiple Access (CDMA) cellular communications radio.
2. Simultaneous operation of 802.11 (a/b/g) and CDMA radios is prohibited by Information Assurance standards, the user shall have the capability to enable/disable the 802.11(a or b or g) or CDMA radios both manually and by firmware.
3. C Model HHRs shall include a National Marines Electronics Association compliant Global Positioning System that will allow handheld applications to capture the latitude-longitude of the handheld at the time transactions are executed on the HHR. The HHR shall be capable of meeting the requirements of Naval Sea Systems Command OP3565 Volume 2 – Hazards of Electromagnetic Radiation to Ordnance (HERO).

b. Additional Separately Orderable Components.

The HHR shall consist of a HHT with pRFID Reader. In addition to the HHR, the HHT shall be orderable as a separate component without the pRFID capability. An upgrade for the HHT to full pRFID capability (including hardware and software/firmware) shall be offered as a separately orderable component. The upgrade shall be user installable or factory installable (at time of order or post field-deployed).

4.2.4.5 D Model, Special Configuration, 902-928 MHz

D Model HHRs shall include all features and components of section 4.2.44 titled Model C, except that it shall be provided with a numeric keypad with keys large enough to be operable by personnel wearing low temperature protective gloves. The numeric keypad shall also have an alternate capability to enter alphabetic data utilizing the numeric keypad. An upgrade for the HHT to full pRFID capability (including hardware and software/firmware) shall be offered as a separately orderable component. The upgrade shall be user installable or factory installable (at time of order or post field-deployed).

4.2.4.6 pRFID Tags

The Government requires pRFID Tags. These Tags will be used in industrial, hazardous, and ordnance environments described in this Part.

- a. The Government requires pRFID tags integrated with Shipping Labels. The Shipping Labels shall be of synthetic label media for use with Thermal Transfer resin ribbon. They shall be provided in roll form suitable for use with the pRFID Enabled Bar Code Label Printer. They shall be provided in 4" by 2" and 4" by 6" label sizes.
- b. The Government requires pRFID tags integrated with labels and optimized for tracking of documents. The Document Tracking labels shall be of paper media for use with Direct Thermal printing (no ribbon). They shall be provided in roll form suitable for use with the pRFID Enabled Bar Code Label Printer.
- c. The Government requires pRFID hardened tags suitable for permanent attachment to office equipment and other assets. The tags shall be hermetically sealed.

- d. The Government requires pRFID hardened tags with an incorporated standoff suitable for permanent use on various materials including metals and containers holding liquids. The tags shall be hermetically sealed.
- e. The Government requires EPC Global Class 3, Gen 2 battery assisted, hardened tags with an incorporated standoff suitable for permanent use on various materials including metals and containers holding liquids. The tags shall be hermetically sealed.

4.2.4.7 pRFID Enabled Bar Code Label Printer.

The Contractor shall provide 902-928MHz and 862 MHz~870 MHz pRFID Enabled Bar Code Label Printers that concurrently print bar codes, text, and graphics, as well as write, read, and verify the Tag's information. The pRFID Enabled Bar Code Label Printers shall have the ability to encode Tag information and print the label utilizing embedded Bar Code Label and Form Design Software. The Contractor shall provide a pRFID Enabled Bar Code Label Printer with the following features and components:

- a. Ruggedized construction;
- b. Concurrently printing bar code symbols, text, graphics, as well as write/read/verify the Tag;
- c. Pre-configured from the factory to print labels and write to/read tags upon delivery;
- d. Easily upgradeable to new firmware revisions;
- e. Print using thermal transfer printing;
- f. Print roll-fed continuous Tags;
- g. Print bar code symbologies with a minimum resolution of 203 dpi;
- h. Print all bar code symbols and densities with at least a Grade A print quality, as defined in ANSI IEEE 802.11g X3.182-1990 (R1995);
- i. Print bar codes and nomenclature in all four of the cardinal directions;
- j. Store User-designed forms and label formats in printer protected memory comparable in size and data content to the DD Form 1387, Military Shipment Label;
- k. Print the linear (with Human Readable Information) and 2D bar code symbologies listed in the paragraph entitled "Bar Code Requirements," in addition to free text, symbols, and graphics;
- l. Have at least the following ports: USB, parallel, IEEE 802.3/Ethernet Network Interface Card with 10BaseT connector supporting TCP/IP;
- m. A minimum four-inch throat size;
- n. Delivered with one 4" wide resin-based printer ribbon;
- o. Delivered with an Operator Maintenance Kit;
- p. Driver support provided for all Microsoft supported versions of Microsoft Operating Systems;
- q. Non-operational Tags shall not be utilized and shall be marked accordingly.

4.2.4.7.1 Separately Orderable Components

The Contractor shall provide the following Separately Orderable Components for the pRFID Enabled Bar Code Label Printer:

- a. Operator's Maintenance Kit;
- b. Replacement Print Head;

4.2.4.7.2 4.1.1.4.2 Consumable Supply

The Contractor shall provide a Resin-based printer ribbon as a Consumable Supply for the pRFID Enabled Bar Code Label Printer.

4.3 pRFID TAG READABILITY REQUIREMENTS

pRFID tags shall meet the following performance requirements as set forth in Military Standard 129P w/Change 4, paragraph 4.9, Passive Radio Frequency Identification (RFID):

- a. The requirement for the palletized unit load passive RFID tags, the pRFID tags on the shipping containers and exterior containers within the palletized unit load, and the UID item unit pack pRFID tags that are passing through a portal, is that the read distance shall be at least 3 meters (3.3 yards), reading passive RFID tags at 10 miles per hour (for example, forklift).
- b. Conveyor. The requirement for an individual shipping container pRFID tag, an individual exterior container pRFID tag, and the UID item pack pRFID tag moving on a conveyor, is that the read distance shall be a minimum of 1 meter (1.1 yards), reading pRFID tags traveling at a speed of 600 feet per minute.

5 SOFTWARE, FIRMWARE, AND SECURITY REQUIREMENTS

5.1 SOFTWARE REQUIREMENTS

5.1.1 Environment

The Contractor shall provide Software that shall support, at a minimum, PCs using Microsoft operating systems. HHRs shall be provided with an industry standard operating system, which allows users to execute applications on the HHR. The operating system on the handheld shall be an Information Assurance (IA) compliant Windows Operating System Win Mobile 6.x or the most current version of the operating system. The Contractor shall provide as a minimum, Configuration/Operational Software to utilize all components that make up the pRFID Class of devices for each technology for the Desktop PCs and HHRs, Software Development Kit license, and Application Development Software. All software offered will include; upgrades, fixes, inherent capabilities, revisions, and peripheral connectivity to maintain the operability, usability, and expansion of the intended software requirement.

5.1.2 Graphical User Interface

All Contractor-provided software for Desktop PCs shall provide a Graphical User Interface (GUI), which shall be the industry-based application software package that supports pRFID technology. The Government requires a GUI that is integrated on the pRFID HHRs.

5.1.3 Capability

All pRFID software shall be provided on CD ROM or DVD. The Government's requirement is to have the necessary software to enable the Government User to perform the technical, functional, and operational requirements of the Passive RFID hardware offered.

5.2 CONFIGURATION / OPERATIONAL SOFTWARE FOR FIXED READER PC

The Contractor shall provide Configuration / Operational Software for PC that, as a minimum, shall provide the Government User with the necessary software utilities to set up, control, and operate the pRFID equipment in actual operational environments. The Government requires software that is user programmable utilizing High Order programming languages. The Contractor shall provide Configuration / Operational Software for PC and shall add, delete, revise, configure, and test Readers / Tags in the operating environment and provide operational status of all pRFID system components and indicate which components need attention, and provide selective addition and deletion of data. pRFID software shall schedule Reader time management and report low battery power conditions for Readers that are battery powered. pRFID software shall perform ad hoc and global searching for specific Tag data stored in a database and subsequently, paste the data into an Microsoft Word or Excel document; manage queried data via database functions; import and export data to database files; and print reports from data gathered from the RFID System, such as manifests, and lists of Tags and Readers present in the operating environment. The Fixed Reader Configuration/Operational Software and all required documentation (in accordance with Paragraph 13, "Documentation Requirements," in Section H) shall be provided to the Government for installation on a PC with the fixed reader and shall not be separately priced.

5.3 CONFIGURATION / OPERATIONAL SOFTWARE FOR HHR

The Contractor shall provide Configuration Software for the HHR that allows the User to manage the pRFID hardware when away from the host computer, which includes data collection pRFID reading and writing to tags, and if wireless communications are included, communication with a host computer. As a minimum, the Configuration Software for HHR shall provide the Government User with the software utilities to set up, control, and operate the pRFID hardware in actual operational environments. The Government understands that some software functions on the HHR are developed as part of the firmware; however, the Government requires the capability to execute code using High Order programming languages. The Configuration Software for the HHR shall add, delete, revise, configure, and test Readers / Tags in the operating environment and provide operational status of all pRFID system components and provide selective addition and deletion of data. pRFID software shall schedule Reader time management and report low battery power conditions for Readers that are battery powered. The HHR Configuration Software shall be installed on the HHR prior to delivery to the Government and shall not be separately priced. All required documentation (in accordance with Paragraph 13 "Documentation Requirements," in this Part D) shall be included and shall not be separately priced.

5.4 APPLICATION DEVELOPMENT SOFTWARE

5.4.1 pRFID Application Development Software

The Contractor shall provide Application Development Software that shall support, at a minimum, PCs with Microsoft supported versions of Microsoft Operating Systems. The Government requires the ability to program, develop, and execute code to support the pRFID Configuration Software. Some of the desired features of the Application Development Software include the ability to download executable code to other devices; tools, libraries, and executive software needed to generate executable code; American Standard Code for Information Interchange (ASCII) file import and export capability; and Structured Query Language capability.

5.4.2 Separately Orderable Components

The Contractor shall provide any special tool kits or utility libraries as Separately Orderable Components.

5.4.3 HHR Software Development Kit

The HHR software development kit (SDK) shall support all of the features of the HHR. SDK libraries provided by the Contractor shall interface with Basic, .NET, and C/C++ language compilers and program development environments. Library routines shall be callable by programs developed with standard languages, including Basic, .NET, and C/C++. The SDK shall include all necessary library routines, run time support, and distribution rights to permit full functionality of developed software using the SDK on all deployed platforms, including scanner/imager, pRFID Reader, screen backlight, and other device-specific features.

5.5 PASSIVE RFID ENABLED PRINTER SOFTWARE

The Contractor shall provide pRFID Enabled Printer Software that combines the features of bar code printing with encoding pRFID embedded labels. The pRFID Enabled Printer Software shall automatically test each RFID label and the encoded data before actually printing the label. If the RFID label is deemed "non-operational," the label shall not be utilized and shall be marked accordingly. The process of verifying each label and printing shall continue with the next "usable" label. In addition, the pRFID Enabled Printer Software shall provide bar code label, form design, and printing software with graphic support, as well as ISO 9075 SQL Call-Level Interface (open database connectivity). The software shall be capable of generating low, medium, and high density bar codes, as well as 2D Symbology (as a minimum, PDF 417, Data Matrix ECC 200, etc.), in addition to free text, symbols, and graphics. The software shall generate the DD 1387 form. The Contractor shall provide software that allows rapid label and form design without requiring the User to learn the complexities of bar code symbologies and printer control languages, displays

a “what-you-see-is-what-you-get” editor for designing bar code labels and forms, and allows viewing of the bar code labels and forms prior to printing. The software shall also permit the use of fixed or variable data for label, form text, and bar codes, and shall import information to be utilized with labels and forms from databases. The pRFID Enabled Printer Software shall execute under all supported versions of Microsoft Windows software and Microsoft Operating Systems. The pRFID Enabled Printer Software shall be supplied preinstalled with the printer and shall not be separately priced.

5.6 FIRMWARE REQUIREMENTS

The Contractor shall provide all necessary firmware required for the operation of the pRFID equipment configuration and components. Firmware shall reflect the baseline configuration and all subsequent Government-approved Engineering Changes. All firmware provided shall be easily implemented by methods determined by the Contractor and approved by the Government. All firmware shall be installed prior to equipment delivery.

6 SECURITY

6.1 HHR AND HHT ACCESS PROTECTION

All HHR and HHT devices shall have the capability to protect access or lock the device.

6.2 SECURITY STANDARDS

All software and hardware provided on the pRFID Contract shall conform to all applicable Army and DoD security requirements to include the requirement that all specified products shall adhere to the requirements of the Unified Capabilities Approved Products List (UCAPL) located at: <https://aplits.disa.mil/> (requires CAC for access). The contractor shall ensure that all contractor personnel accessing information systems are properly trained and certified as required by DFARS Clause 252.239-7001. The Contractor shall comply with the following standards, and Government guidelines to include all new versions, amendments, and modifications made to the listed documents and standards, as applicable.

- a. Office of Management and Budget (OMB) Circular No. A-130 Revised, (Transmittal Memorandum No. 4) Management of Federal Information Resources – Appendix III, Security of Federal Automated Information Resources, 28 November 2002.
- b. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 140 – 2, Security Requirements for Cryptographic Modules, 25 May 2001, w Change Notices 12-03-2002.
- c. DoDD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG), 14 April 2004.
- d. Assistant Secretary of Defense Memorandum, Use of Commercial (WLAN) Devices, Systems, and Technologies in the DoD GIG, 02 June 2006.
- e. DoDD 8500.01E, IA, 24 October 2002, current as of April 24, 2007.
- f. DoDI 8500.2, IA Implementation, 06 February 2003.
- g. DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), November 28, 2007.
- h. Army Regulation (AR) 25-2, IA, 23 March 2009.
- i. Best Business Practice 03-EC-M-0003, Wireless Security Standards, Version 2.0, 15 June 2007.
- j. DFARS Clause 252.239-7001.

After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the listed standards.

6.3 DOD INFORMATION ASSURANCE REQUIREMENTS

All devices and/or systems provided by the Contractor that receive, process, store, display or transmit information shall comply with the applicable IA requirements specified in DoDD 8500.1E, *Information Assurance (IA)* (reference g) and DoDI 8500.2, *Information Assurance (IA) Implementation* (reference h).

Examples of systems which must meet these IA requirements include but are not limited to: stand-alone information systems; networked computers and servers; mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode; and other information technologies as may be developed and/or proposed by the Contractor.

6.4 DOD WIRELESS DEVICE SECURITY REQUIREMENTS

pRFID implementations that utilize IEEE Standard 802.11 WLAN products to store, process, or transmit unclassified information shall comply with the requirements specified in Assistant Secretary of Defense Memorandum, Use of Commercial WLAN Devices, Systems, and Technologies in the DoD GIG (reference d).

6.5 ARMY WIRELESS DEVICE SECURITY REQUIREMENTS

Army pRFID implementations that utilize IEEE Standard 802.11 WLAN products or other wireless technologies to store, process, or transmit unclassified information shall comply with the applicable requirements specified in AR 25-2, *Information Assurance* (reference h) and Army Best Business Practice 03-EC-M-003, *Wireless Security Standards* (reference i). Other Services (e.g., USAF, USN) pRFID implementations that may include wireless devices will have the security requirements stated in the individual contract order.

6.6 COMMON CRITERIA COMPLIANCE REQUIREMENTS

Common Criteria compliance is determined and verified by favorable product testing against a CCPP. CCPPs are developed under sponsorship of the National Security Agency (NSA). Common Criteria tests are conducted by a Common Criteria Test Laboratory (CCTL) that has been approved and accredited by the National Information Assurance Partnership (NIAP). NIAP is a partnership agreement between NSA and the NIST. No such CCPP currently exists for pRFID technology. Therefore, upon approval and adoption of a CCPP for pRFID technology, the Contractor shall no later than six months after the adoption of a relevant CCPP submit product(s) with documentation to a designated CCTL for Common Criteria testing. Subsequently, only products tested and compliant at the Medium Robustness level (as defined in the CCPP standard) shall be permitted through this Contract. Information regarding Common Criteria Compliance can be obtained from the following web site: <http://www.commoncriteriaportal.org/>.

6.7 SECURITY CERTIFICATION AND ACCREDITATION SUPPORT

The Contractor shall support all Government efforts to obtain Certification and Accreditation (C&A) for the products provided under this Contract in accordance with the guidance contained in the *Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance* (reference j) and DoD Instruction 8510.bb, *DoD Information Assurance Certification and Accreditation Process (DIACAP)* (reference i). In support of the Government's C&A activities, the Contractor shall provide copies in vendor format of component design specifications, component user manuals, results of any security tests already completed, and component vulnerability assessments. For testing in support of certification and accreditation, the Contractor shall provide the Government with access to Contractor personnel involved with design, engineering, operations, and security attributes of the products.

6.8 SECURITY MAINTENANCE SERVICES

The Contractor shall ensure that the devices and/or systems provided under this contract comply with all new versions, amendments, and modifications made to the security documents and standards cited in this Contract, when applicable and commercially available. To ensure continued compliance, the Contractor shall perform the necessary configuration changes, as approved by the Government. These configuration changes may include, but are not limited to: performing system configuration changes, installing patches and bug fixes; conducting hardware/software upgrades, updates, and replacements.

6.9 GOVERNMENT EVALUATION

The Contractor shall support Government compliance verification evaluation and security certification and accreditation of the products provided under this Contract. The Government will coordinate the scheduling of any evaluation with the Contractor. The Contractor shall cooperate with Government personnel and

Government representatives who plan, conduct, and report any Government testing. Support of Government testing, when requested, includes Government or its agents access to Contractor facilities, documentation, and/or personnel used by the Contractor to produce the products provided under this Contract. The Contractor shall assist in resolving any problems resulting from the Government verification evaluations and security certification and accreditation process. This shall address problem reports, technical investigations, and any testing performed.

6.10 CYBERSECURITY DOCUMENTATION REQUIREMENTS

- a. The contractor shall support Government Information Assurance (IA), Certification and Accreditation (C&A), and Connectivity or Interconnectivity activities as required, including providing C&A documentation, upon request, in a format acceptable to DoD IA and C&A activities.
- b. The contractor shall report all IAVAs, STIGs and Bulletins within a system Plan of Action and Milestone (POA&M) at least monthly and provide a list outlining which were implemented, those not implemented and why they were not and how mitigated if mitigation required. All non-implemented IAVAs and STIGs shall have Government concurrence. The contractor shall provide a comprehensive and up to date software scan using current Army Best Business Practices for scanning and remediation every month. This data will be rolled up to the ASAALT Cyber and the PEO to ensure the basic mission assurance techniques are implemented uniformly with the portfolio.
- c. The contractor shall perform manual scans and provide to the Government at least monthly to ensure the system is Federal Information Security Management Act (FISMA) and Security Technical Implementation Guide (STIG) compliant.

6.11 UPDATES, INCIDENT REPORTING AND VULNERABILITIES MANAGEMENT

6.11.1 IAVAs

- a. The contractor shall apply Exploit category A IAVAs within 14 days of notification through the NETCOM SharePoint site.
- b. The contractor shall apply Exploit category B IAVAs within 14 days, when possible, or within 30 days if a system level POA&M to mitigate is provided.
- c. The contractor shall monitor all update requirements including but not limited to (vendor sites, mailing lists, third party sources, vulnerability scans and US Army Network Enterprise Technology Command (NETCOM) SharePoint site for Information Assurance Vulnerability Messages.) The contractor shall make mitigation, patching, upgrade or modification recommendations and provide a Plan of Action and Milestones (POA&M) for all requirements that cannot be fulfilled on time, in a format approved by the PEO for each update requirement. The contractor shall treat the POA&M as specified in the system's security classification guide (SCG) and provide a digital copy to the Government via a method approved the Government. The contractor shall provide a comprehensive and up to date software scan using current Army Best Business Practices for scanning and remediation every month.

6.11.2 Security Technical Implementation Guides (STIG)

Contractor shall implement STIGs within 30 days from release of a new DISA STIG. Where an update cannot be technically applied due to system functionality, that STIG item shall be documented in the system POAM with appropriate mitigations. If an update cannot be applied within 30 days the contractor shall provide a milestone schedule in the POAM item for application for Government approval.

6.12 DESIGN CONSIDERATIONS

The contractor shall develop a cyber-resilient system by ensuring IAVAs and STIGs can be applied individually without the need to re-image the system, and not only update IAVAs or STIGs during new capability updates.

1. DOD Instruction 8500.2, Information Assurance (IA) Implementation, definition.

2. ARCYBER Situational Awareness Report 2014-004, Establishment of the Exploit Categorization of Information Assurance Vulnerability Alerts, definition

7 MANAGEMENT

The requirements found in this section 7 Management, shall not be separately priced.

7.1 pRFID PROGRAM MANAGEMENT

a. The Contractor shall provide the following pRFID Program Management activities and services:

1. Two-work day response to program issues and problems associated with the execution of the Contract as identified by PD AMIS;
2. Support by means of Electronic Commerce/Electronic Document Interchange (EC/EDI), web access for Contractor-provided information and data;
3. Maintain accurate records
4. Provide response within one workday to questions or problems;
5. Provide information to various Services and Agencies with the approval of PD AMIS;
6. Receive and process customer DOs, purchase card orders, and TOs;
7. Develop, update, and maintain the User Guide as per CDRL A002;
8. Coordinate shipments and deliveries;
9. Report order and delivery status as per CDRL A001;
10. Provide the requisite Repair Center(s) (RC) to perform all warranty and maintenance services required by this Contract;
11. Maintain warranty and maintenance records;
12. Provide access for pRFID Users to an identified database location for this Contract;
13. Develop and execute a management plan that incorporates configuration management and risk management, and provide a pRFID Management Plan as per CDRL A003;
14. Schedule project reviews and internal seminars and conferences, and present Contractor's vision of new technology;
15. Schedule and perform demonstrations;
16. Conduct monthly Project Progress Reviews (PPR) year 1 and quarterly thereafter as per CDRL A004;
17. Provide Status Reports to include Warranty Status Reports as per CDRL A009;
18. Provide Monthly Equipment and Service Reports (MESR) as per CDRL A008.
19. Report Contractor Manpower Information in accordance with the paragraph entitled "Contractor Manpower Reporting" in section 7.3.4.

b. The Government desires Contractors, and their respective subcontractors, teaming partners and commercial manufacturers who hold and maintain commercial quality certifications, e.g. ISO certifications, Lean Six Sigma, Capability Maturity Model Integration (CMMI), over the life of the Contract.

7.1.1 Points of Contact

The Contractor shall provide a list of Contractor points-of-contact to the COR no later than ten workdays after the effective date of the Contract. The list shall include names, telephone numbers, facsimile numbers, e-mail addresses, and areas of responsibility for the pRFID Contract. The Contractor shall notify the COR no later than five workdays of replacement of a point-of-contact.

7.1.2 pRFID II Contract Program Manager

a. The Contractor shall identify to the Government a Program Manager for the pRFID II Contract as per CDRL A012. The Program Manager shall at no additional cost to the Government be available with a 24 hours' notice to meet with the Government at the Hoffman II Building located at 200 Stovall Street, Alexandria, Virginia 22332-0022. The pRFID II Contract Program Manager shall address and resolve

pRFID II programmatic issues, facilitate information exchange with the Government, and enhance management coordination.

- b. The Contractor's pRFID II Program Manager shall manage all DOs/TOs, and purchase card orders, and shall be the Contractor's authorized point-of-contact for the PD AMIS, the COR, and the point-of-contact for DOs/TOs and purchase card orders as per CDRL A012. The Contractor's pRFID II Program Manager shall be responsible for formulating and enforcing work standards, assigning schedules, and reviewing work discrepancies, communicating policies, purposes, and goals of the organization to the assigned Contractor personnel for performance of this Contract. The Contractor's pRFID II Program Manager shall manage DO and TO performance.

7.2 USER GUIDE

7.2.1 Purpose

The Contractor shall develop and provide to the Government a User Guide (UG), to assist Government personnel in determining the system configuration that will best meet their Passive RFID operational requirements. The Contractor shall provide the UG no later than 90 calendar days after issuance of the Contract effective date specified in the Notice to Proceed and be available to Users on the Contractor's web site. The UG shall be a comprehensive tool that aligns with the Attachment 0004, SECTION B, Pricing Guide/SLIN Listing to enable prospective Users to formulate a workable process as to potential solutions utilizing the SLINS within the Contract which best meets their operational requirements.

7.2.2 User Guide Review

The Contractor shall provide a draft UG electronically to the COR of the PD AMIS, and KO for review no later than 30 calendar days after issuance of the Contract effective date specified in the Notice to Proceed. The KO will either approve the UG or provide comments to the Contractor for incorporation into the UG. The Contractor shall then have 15 workdays to edit the UG based on Government comments. Upon Government acceptance and approval by the KO of the draft, the Contractor shall make the UG available to Users on the Contractor's web site.

7.2.3 User Guide Approval and Posting

The initial UG must be approved by the KO prior to making the UG available to the Government personnel on the Contractor's web site. Subsequent UG revisions resulting from a formal Contract modification shall be made available to the Government personnel on the web site no later than five workdays of issuance of the Contract modification. The Contractor shall update the UG for other changes (e.g., Government points of contact) within five workdays after the receipt of a request from the COR. The Contractor shall post Contractor-related administrative changes within five workdays of the change.

The UG shall be divided into logical sections for ease of use. The sections shall provide a User with a complete User list, with a detailed description of features and prices for User of all hardware, hardware cables, software, user procedures, recommended equipment configurations, TES, training, warranty, maintenance, CLIN price list, and any additional information that the Contractor includes to simplify the implementation of a Passive RFID solution. The UG shall be a simple, easy to understand document that allows Users to order and build configurations that meet their needs. The Contractor shall provide access for authorized Government Users with ".MIL" email addresses to the UG via the World Wide Web.

7.2.3.1 Sections

Each section of the UG shall be technically accurate, align with the Pricing CLIN structure and complete with descriptions of the hardware (to include pictures), software, and technical engineering services. CLINs shall be used throughout the document to facilitate the User's ability to properly identify and order the appropriate item(s). CLINs shall be clearly annotated on drawings, charts, product descriptions, specification sheets, etc. When a product requires additional equipment to make a complete workable

product, the additional equipment and CLINs, if applicable, shall be clearly identified in the description. All references to a geographic area where products may, or may not, be used shall be clearly annotated in the UG and the CLIN description, if applicable. The UG shall include, but not be limited to, the sections identified below which address the minimum requirements for each Section.

7.2.3.2 Hardware

The hardware section shall be organized into sub-sections based upon the major types of equipment provided, and shall include a discussion of the main features of each piece of equipment, including physical dimensions, power requirements (wattage and voltage), and heat generated by equipment. Precautions, such as the minimum distance between various devices, shall be provided. The UG shall contain instructions for the User to specify equipment destination to ensure the pRFID equipment is compatible with the commercial power supply and adapter plugs for the geographic area in which it will be operated.

7.2.3.3 Hardware Cables

This Section shall list all cables with Model Numbers provided and equipment cable requirements in a chart format that shall allow the User to identify the correct cables for connecting pRFID devices. CLINs shall be provided on the chart. All cable requirements for equipment installation shall be described in this section. This Section shall clearly indicate the appropriate cables and interfaces for the various pRFID components and provide a reference to the applicable parts.

7.2.3.4 Software

This section shall provide a full description of all software CLINs provided that include a discussion of the primary function, minimum memory requirements, program capabilities, and major features and benefits. This section shall explain, in non-technical terms, the recommended software packages for specific applications. The Contractor shall maintain an asset record showing the software version and configuration installed on all shipped products. The Contractor shall track and update the asset record when the Contractor makes changes to products and product software when returned for service or when changes are made by the Contractor on fielded systems.

7.2.3.5 User Ordering Procedures

This section shall contain ordering procedures that provide the User with all the necessary information required to order pRFID products and TES. Contractor points-of-contact, telephone numbers, Help Desk access, and addresses shall be included.

7.2.3.6 Recommended Equipment Configurations

This section shall address the Contractor's recommended equipment configurations to meet various Users' pRFID requirements with easy to understand, step-by-step directions, and any physical or facility considerations. The recommended configurations shall represent the most economical hardware, software, and technical engineering services that meet possible User requirements. This section shall provide information to assist the User's with building a pRFID configuration that best meets their needs. The configurations shall include the appropriate CLIN numbers.

7.2.3.7 Technical Engineering Services

This Section shall contain procedures that provide the User with all necessary labor categories available with their fixed labor rates information required to estimate and order TES. All TES CLINs identified shall be addressed in this Section.

7.2.3.8 Training

This Section shall provide type of Training available and suggested as part of a passive RFID implementation.

7.2.3.9 Warranty

This Section shall address all warranty provisions of the Contract i.e., how to obtain warranty service, Help Desk telephone number and hours of operation, warranty repair sites, RMA issue procedure etc.

7.2.3.10 Maintenance

This Section shall describe the various maintenance services available to User worldwide with CLIN prices, how to order maintenance services, and Help Desk instructions for User maintenance support.

7.2.3.11 CLIN Price List

This Section shall provide the contract CLIN Price List with products and services provided for each CLIN/SLIN. The CLIN Price List will be updated within five days of addition or deletion of a CLIN/SLIN on contract.

7.3 pRFID MANAGEMENT PLAN

The Contractor shall provide a pRFID Management Plan. The Plan shall be submitted to the COR no later than 30 calendar days after issuance of the Contract effective date specified in the Notice to Proceed. The PD AMIS will either approve the Management Plan, or provide comments to the Contractor for incorporation into the Management Plan. The Contractor shall then have 10 workdays to incorporate the Government's comments into the Plan, and resubmit the Plan to the COR. The Contractor shall manage the Contract in accordance with the Government-approved pRFID Management Plan. The pRFID Management Plan shall include, but not be limited to the following:

- a. Management and Reporting Methodology for Gathering, Validating and Generating Reports;
- b. pRFID Configuration Management Plan (see Paragraph PWS 7.4 for separate CM Annex / deliverable);
- c. Risk Management;
- d. Repair Center Approach;
- e. Integrated Process Team (IPT) Methodology;
- f. Electronic Commerce and Electronic Data Interchange Methodology;
- g. Web Site Methodology;
- h. Training Development and Support;
- i. Technology Assessment and Control;
- j. Logistics Support to include the Contractor's approach to satisfying unusual or surge requirements and to deal with crises.

7.3.1 Integrated Product Teams

The Contractor shall participate with the Government on pRFID Integrated Product Teams (IPTs) and provide minutes of the meetings no later than five workdays after each meeting. IPTs will be composed of representatives from all functional disciplines, working together to identify and resolve issues. IPTs will also make sound and timely decisions, build a successful and balanced program, and make maximum use of timely input from the entire Team, including customers and suppliers.

7.3.2 Project Progress Reviews

The Contractor shall conduct Project Progress Reviews (PPRs) for Government personnel at a mutually agreeable facility. PD AMIS will schedule the initial PPR. It is anticipated that the first PPR will occur no later than 90 calendar days after the Contract effective date specified in the Notice to Proceed. Thereafter, PPRs shall occur on a monthly basis for the next twelve months of the Contract, and quarterly thereafter, for the life of the Contract. During each PPR, the Contractor shall present material that addresses:

- a. Status of current technological substitutions and additions;
- b. Status of configuration and risk management activities;
- c. Status of TOs/ DOs and purchase card orders, to include but not limited to, received and processed dates (listed by ordering agency), scheduled delivery date, and shipped date;
- d. Actions under warranty and maintenance;
- e. Significant trends (quantities by CLIN, component reliability safety issues, problems, and recommended solutions);
- f. Minutes from the previous PPR;
- g. Activities determined to be of importance to the Government, such as unanticipated problems, and high visibility issues identified by the Government;
- h. Status of significant program events;
- i. Customer feedback;
- j. Agencies and organizations contacted and initiatives with each;
- k. Reason for delinquent TOs/ DOs, and purchase card orders.

The Contractor shall include in each review, a current organizational chart that includes the names and telephone numbers of all key personnel proposed and included with the pRFID contract, or as may be proposed and used in securing subsequent TOs. All changes to key personnel changes are to be identified at the time changes are known and explanation included for how the contractor shall minimize impact of such changes. Key personnel for this Contract are Senior Information Systems Engineer; Project Manager; Senior Programmer performing on TOs; and the Contract Program Manager.

The Contractor shall prepare and coordinate with the COR, an agenda for all PPRs at least five workdays before a scheduled PPR. The Contractor shall provide the briefing charts to the COR electronically three workdays prior to the day of the PPR. The Contractor shall prepare and coordinate minutes of the PPRs with PD AMIS no later than five workdays after the PPR. Coordination shall be accomplished through electronic mail. Upon PD AMIS approval, the Contractor shall, no later than five workdays, post the minutes on the web site specified in the paragraph "Web Site" in this Part. The Contractor shall hotlink the web site to the PD AMIS web site.

7.3.3 Status Report

The Contractor shall prepare and submit a Status Report in Microsoft Office Excel format, monthly as per CDRL A005. The report shall include all orders placed by the Government and by Government Contractors (reference the paragraph "Government Contractor's Use of Contract" in Government Contracting Officer's Ordering Guide during the reporting period. The Contractor shall submit the first report to the COR on the 10th day of the month following the one-month period after the Contract effective date specified in the Notice to Proceed. The Contractor shall submit subsequent reports in monthly increments on the 10th day of the month following the reporting period throughout the performance period of the Contract. The report shall include, as a minimum, a list of all equipment delivered by:

- a. CLIN, with brief description, by month, by Service or Agency, total quantities and dollar amount;
- b. Year-to-date, total quantities and dollar amount;
- c. Contract-to-date, total quantities and cumulative dollar amount;
- d. The totals for each category (above) shall also reflect the values for products/equipment and services in a summary table.

An example report format is located at Exhibit B in this Part.

7.3.4 Contractor Manpower Reporting (CMR)

The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collection site where the Contractor shall report ALL Contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the pRFID-II Contract via a secure data collection site. The Contractor is required (as per CDRL A013, Sect. J, Attachment 006) to completely fill in all required data fields using the following web address: <http://www.ecmra.mil>, and then click on "Department of the Army CMRA" or the icon of the DoD organization that is receiving or benefitting from the contracted services.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2013. Contractors may direct questions to the help desk by clicking on "Send an e-mail" which is located under the Help Resources ribbon on the right side of the login page of the applicable Service/Component's CMR website. Contractors may use a direct XML data transfer to the data base server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractors system to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the website.

The required information includes:

- 1) Contracting Office, Contracting Officer, Contracting Officer's Technical Representative;
- 2) Contract number, including task and Delivery Order number;
- 3) Beginning and ending dates covered by reporting period;
- 4) Contractor name, address, phone number, email address, identity of Contractor employee entering data;
- 5) Estimated direct labor hours (including sub-Contractors);
- 6) Estimated direct labor dollars paid this reporting period (including sub-Contractors);
- 7) Total payments (including sub-Contractors);
- 8) Predominant Federal Service Code (FSC) reflecting services provided by Contractor (and separate predominant FSC for each sub-Contractor if different);
- 9) Estimated data collection cost;
- 10) Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army Requiring Activity is responsible for providing the Contractor with its UIC for the purposes of reporting this information);
- 11) Locations where Contractor and sub-Contractors perform the work (specified by zip code in the United States and nearest city, country, when in an overseas location, using standardized nomenclature provided on the website);
- 12) Presence of deployment or contingency Contract language; and
- 13) Number of Contractor and sub-Contractor employees deployed in theater this reporting period (by country).

7.4 CONFIGURATION MANAGEMENT

7.4.1 pRFID II Configuration Management Plan

The pRFID equipment shall be configuration-controlled, accounted for, and audited in accordance with the Contractor developed and Government-approved, pRFID Configuration Management Plan as per CDRL A006. The Contractor shall provide the pRFID Configuration Management Plan as an Annex to the pRFID Management Plan, which shall be submitted to the COR for approval no later than 30 calendar days after issuance the Contract effective date specified in the Notice to Proceed. The pRFID Configuration Management Plan shall reflect best commercial practices and shall be in accordance with accepted industry standards. The Contractor shall submit the initial Baseline with the Configuration Management Plan. The baseline matrix shall include, at a minimum: Equipment Nomenclature, Manufacture Model Number,

Manufactures Part Number Firmware Version, Date of Implementation, Software Version, Relevant Specification Paragraph, and any constraints. The matrix shall be in Microsoft Office Excel format. Any changes in hardware or software will be a change to the baseline and will require Government approval. Once changes to the baseline are reviewed and approved by the Government the Contractor shall provide configuration updates to the UG showing changes in hardware and software versions, date of change, and other nomenclature.

Plan shall define those instances when the Contractor shall notify the Government of pending changes to the pRFID Equipment Baseline Configuration.

7.4.2 Changes and Modifications

All OEM changes prior to Contract award shall be included in equipment provided under this Contract at no additional cost to the Government. The Contractor shall notify the KO of all OEM-sponsored changes to any equipment provided on the Contract. All changes shall be provided to the Government at least 45 calendar days prior to implementation for evaluation and will be subject to the KO's approval before the changed products may be placed on the Contract.

7.4.3 Changes to Software

The Contractor shall notify the KO of all changes to the software and documentation provided under the Contract throughout the warranty period, including any software updates and upgrades (for example, bug fixes, new features, enhancements, and revisions) as they become available. Software changes are defined as any software product and documentation which is provided for any other customer free of charge, or which the software manufacturer does not consider a new product. Changes to firmware, software or documentation (e.g., User Manuals) (including packaging and shipping) shall be provided at no additional cost to the Government.

7.4.4 Notification of Software Changes

The requirement for any software change involving a change to form fit or function is that the Contractor shall provide PD AMIS one copy of the changed software with documentation (e.g., User Manuals) for each affected software item previously accepted by the Government. Any changes to the baseline will require the contractor to perform all functions detailed in approved configuration management plan to ensure that any changes to the software or firmware will not affect performance, security requirements, safety, NI, Hero, and other requirements within this Statement of Work (SOW). After Government evaluation of the changed software, the KO will notify the Contractor of the acceptance or rejection of the latest release. Software changes not involving a change to form fit or function shall be provided to the Government on the Contract after notification is provided to the KO.

7.4.5 Correction of Safety Hazards or Equipment Malfunctions

In accordance with commercial practices, the Contractor shall notify the KO and PD AMIS of all OEM-sponsored changes to correct safety hazards or equipment malfunctions. The Contractor shall implement changes to correct safety hazards in accordance with commercial practices. The implementation shall be in accordance with a mutually agreed-upon schedule. All such changes shall be implemented at no additional cost to the Government.

7.4.6 Configuration Audits

The Government is required to maintain configuration control over functional and performance requirements (form, fit, and function). Subject to the issuance of a TES TO, the Contractor shall support the Government in performing Functional Configuration and Physical Configuration Audits. The Contractor shall provide a demonstration of the equipment. At least seven workdays prior to commencement of the equipment demonstration, the Contractor shall deliver a Demonstration Plan to the Government. The Plan shall include the agenda, demonstration procedures, and a matrix identifying the

baseline equipment. The baseline matrix shall include, at a minimum: Equipment Nomenclature, Model Number, Firmware Version, Software Version, Relevant Specification Paragraph, and any constraints. The matrix shall be in Microsoft Office Excel format.

7.4.7 Physical Configuration Audit

A Physical Configuration Audit (PCA) is the formal examination of the “as-built” configuration of a commercial item against its technical documentation to establish or verify the commercial item’s product baseline.

7.4.8 Functional Configuration Audit

A Functional Configuration Audit (FCA) is the formal examination of the functional characteristics of a configuration item to verify that the item has achieved the requirements specified in its functional and allocated configuration documentation. The FCA is performed by the Government’s Configuration Management Team or Quality Control Representative, by auditing the requirements specifications against the pRFID Contractor specifications of each configuration item (hardware, middleware, and software).

7.5 RISK MANAGEMENT.

Risk Management is an essential part of program management. The Contractor shall continually identify, assess, manage, and control project risks as per CDRL A007. The objective is to reduce program uncertainties, and to classify risks according to their probability of occurrence, and possible consequences. In accordance with the Government-approved Management Plan, the Contractor shall identify project risks or actions that affect the accomplishment of program objectives. The program risk events include, but are not limited to the following:

- a. Technical performance;
- b. Operational performance;
- c. Schedule performance;
- d. Training;
- e. Technical standards;
- f. Logistics readiness.

The Contractor shall prioritize project risks and determine the status of risk reduction or mitigation efforts. The Contractor shall report the status of risk management efforts during the PPRs.

7.6 MONTHLY EQUIPMENT AND SERVICE REPORT

The Contractor shall provide PD AMIS, the COR, and KO with a Monthly Equipment and Service Report (MESR) in Microsoft Office Excel format via electronic mail and post it on the Contractor’s web site for on-line viewing and ad hoc inquiries by authorized Users. The initial MESR shall be submitted covering the month the first pRFID item is received by the Contractor for repair (warranty or maintenance), and shall be provided no later than 10 calendar days after the end of each subsequent month (e.g., January report is due by 10 February). The Contractor shall provide, as part of the MESR, a consolidated list of service User calls for troubleshooting assistance. This detailed information for warranty and maintenance repairs will be used to identify trends and compliance with equipment turn-around requirements. The MESR shall include a separate line item of description for each pRFID item service incident and, as a minimum, shall include the following:

- a. Return Material Authorization (RMA) number and date assigned to User Category of service action: Per-incident maintenance, On-call maintenance or Warranty;
- b. Identify if User requests same serial number item returned. Also, note if User changed their mind because of time delay in receiving the same serial number in return;

- c. Identity of the Federal agency (that is, Army, Navy, DLA, etc.), Government User and Point of Contact (POC), and site requiring the maintenance;
- d. Parts breakout: nomenclature; National Stock Number (NSN), if available; part numbers; model number, CLIN; and serial number;
- e. Quantity of each type of component repaired or replaced by CLIN under the Contract to date;
- f. Equipment Warranty expiration date;
- g. DO number or purchase card order date and activity;
- h. Date field engineer arrival on-site, or receipt of the failed pRFID equipment at the repair facility;
- i. Date repair action was completed, or equipment was sent back to the User, shipper or carrier, or when picked up by the User;
- j. Remarks section providing information outside of the items listed above, which gives a brief, non-technical description of equipment problems identified, repair action accomplished, parts replaced, serial numbers of replacement pRFID items (if the item was replaced by the Contractor), problems identified but causes not isolated, or a statement of no evidence of failure.

7.7 WARRANTY STATUS REPORT

The Contractor shall provide a Warranty Status Report in Microsoft Office Excel format, once each Contract year as requested by the COR, to include but not limited to, a list of all equipment due to leave warranty status no later than the next twelve months with serial number, model number, Federal Agency, Unique Control Number, DO number, shipping date, warranty end date, Government User, point of contact and telephone number. The initial report format shall be provided by the Contractor for Government review and approval no later than 30 calendar days after issuance of the Contract effective date specified in the Notice to Proceed.

8 REPAIR REQUIREMENTS

8.1 REPAIR CENTERS

The Contractor shall provide a Repair Center(s) (RCs) to be operational no later than 90 calendar days after the first DO is issued. The Contractor shall repair or replace failed equipment, provide on-call and mail-in repair, and provide technical assistance to the Users. The Contractor shall provide maintenance personnel who have maintenance experience on the pRFID equipment. The maintenance personnel shall have obtained experience with the pRFID configurations prior to their assignment to the pRFID Contract. All Contractor personnel providing assistance shall understand and speak fluent English.

8.1.1 Points of Contact

The Contractor shall provide the KO and the COR with the POC, telephone numbers, facsimile numbers, e-mail addresses, and mailing addresses for each RC. The Contractor shall provide updates to the Government as changes occur.

8.1.2 RC Hours of Operation

The RC(s) shall be operational between the hours of 8:00 A.M. through 5:00 P.M., local time, Monday through Friday. This excludes U.S. Federal and Host Nation Country holidays in the geographic location of the RC.

8.1.3 Equipment Return and Tracking

The Contractor shall affix a label to all hardware items deemed appropriate by the Government offered under the pRFID II Contract that states the Contractor's name, help desk phone number and website for warranty and maintenance tracking. The Contractor shall provide a method to enable the Government User and the Contractor to quickly identify and track components being forwarded to, and returned from, the

Contractor RCs for warranty and maintenance services. The Contractor shall assign the User a RMA number prior to the Government mailing-in the failed equipment to the RC for repair or replacement. The User shall be informed of the RMA number and serial number of each component returned to the Contractor for warranty and maintenance service. All failed equipment returned to the RC shall be identified by the RMA number. The RMA number will be used by the Government to help track the failed component through the warranty or maintenance service process.

9 CUSTOMER SUPPORT.

Customer Support shall not be separately priced and shall be provided as per CDRL A010.

9.1 TECHNICAL ASSISTANCE

The Contractor shall provide Technical Assistance, as follows:

- a. Troubleshooting and correction of equipment problems;
- b. Processing requests for On-call Maintenance;
- c. Processing Mail-in warranty and maintenance service issues; for example, assigning RMA numbers;
- d. Providing Contractor address of the RC(s).

9.1.1 Toll-Free Customer Support Help Desk

The Contractor shall provide toll-free telephonic support for a Customer Support Help Desk in CONUS and OCONUS. The Help Desk shall be staffed 24 hours a day, 7 days per week, except when U.S. Government holidays and OCONUS Host Nation holidays coincide. The Help Desk shall respond to the User's call no later than 4 hours after receiving User call 95% of the time, maintain a database of calls received and acted upon, and track User calls for troubleshooting assistance. Except for the purpose of leaving a phone number for the Contractor to return a call no later than one hour during periods of high call volume, recorded answering services are not acceptable to the Government; however, the Contractor may use an on-line knowledge base, and an on-line RMA input functionality to assist Help Desk staff meet the workload. Contractor personnel staffing the Customer Support Help Desk shall possess sufficient expertise to recommend troubleshooting procedures and possible corrective actions for equipment and software acquired under the pRFID Contract. Contractor personnel staffing the Help Desk shall understand and speak fluent English. The Contractor shall maintain records of User calls for troubleshooting assistance capturing the following: failed item POC, location, date, problem, and resolution. This information shall be provided in the MESR.

9.1.2 Web Site

The Contractor shall establish and maintain a worldwide web site for Government Users no later than 60 calendar days after the Contract effective date specified in the Notice to Proceed as per CDRL A011. The web site shall be hot linked to the PD AMIS web site and be available daily on a 24-hour basis, until the expiration of the last active Order issued under the Contract. The web site shall not be password protected and shall only be accessible from a .mil or .gov web domain. As a minimum, the Web site shall include, or provide hotlinks to the following:

- a. Methods for User to track status of DOs/TOs using the Government's order number and a Unique Control Number;
- b. Warranty and maintenance tracking using the RMA number;
- c. Exchange of technical information between the Contractor and individual User and groups;
- d. POC, telephone and facsimile number, email address and mailing address for each RC;
- e. Technical troubleshooting support;
- f. Failed equipment tracking and status;
- g. User Guide;
- h. Reference and User Manuals (i.e., Commercial Manuals, Technical Manuals, Software Manuals);

- i. Project management reports (schedules, IPT and PPR minutes, etc.);
- j. Recent news items from PD AMIS or the Contractor (eg.,, notifications of the web site being down for maintenance);
- k. Other data as mutually agreed to by the Government and the Contractor;
- l. Passive RFID device drivers;
- m. Monthly Equipment and Service Report, Status Report, and Warranty Status Report; and
- n. List of products that fully comply with Section 508 of the Rehabilitation Act.

The Contractor shall ensure that all device drivers required to operate pRFID equipment are posted to the web site. At a minimum, the Contractor shall post to the web site those drivers that were developed by the Contractor for use under this Contract. All initial drivers shall be posted to the web site no later than 60 calendar days after the Contract effective date specified in the Notice to Proceed. New and updated drivers shall be posted to the web site no later than 48 hours of the COR's approval. In the event that drivers are updated, the original version shall also be maintained on the web site.

10 WARRANTY

The Contractor shall provide a minimum of a three-year warranty and offer options for the government to procure extended warranties¹ for four years and five years at the time of product purchase. All warranties shall include all parts, labor, and transportation costs for all pRFID components provided under this Contract. The Contractor shall provide a minimum of a three-year warranty for all software products with options for the government to procure software products with a four-year warranty and with a five-year warranty. The Contractor shall repair or replace all failed pRFID components covered under warranty in this Contract in accordance with the procedures described in the Warranty Support paragraph. All warranties shall be included in the purchase price of the component, and not priced separately. The Contractor shall immediately notify the ordering KO and order POC regarding equipment requiring repair or replacement due to apparent User abuse, negligence, or missing significant parts, such as circuit cards or boards.

10.1 WARRANTY SUPPORT

During the equipment warranty period, the Contractor shall implement changes to correct equipment malfunctions in accordance with best commercial practices. The implementation shall be in accordance with a mutually agreed-upon schedule. These changes shall be made at no additional cost to the Government. The warranty shall fully protect the Government against equipment malfunctions due to material defects, workmanship, or intrinsic operating problems. The warranty period for items ordered by DO shall begin upon Government acceptance of the equipment. In the event the Contractor is authorized to use a Certificate of Conformance, the warranty period for items ordered by a DO shall begin on the date of shipment. The warranty period for items ordered by purchase card shall be in accordance with the paragraph entitled "Governmentwide Commercial Purchase Card" in Government Contracting Officer's Ordering Guide. The warranty shall include mail-in procedures and on-call procedures as specified below.

10.2 WARRANTY MAIL-IN PROCEDURES

The requirement for warranty mail-in service, including commercial carriers, is that the Contractor shall bear all shipping costs, both from and back to Government sites. The Contractor shall be responsible for the equipment from the time of receipt until safe return to the Government. The Government will provide the Contractor with any unusual transportation instructions for return shipment after repair. When the User does not require the same serial number equipment, the Contractor shall ship a replacement item no later than 24 hours after notification of failed pRFID components. If the User requires the same serial number equipment, the Contractor shall restore all malfunctioning equipment covered under warranty to an operational condition and ship the equipment back to the User no later than ten workdays after receipt of

¹ Extended warranties timeframes reflect total duration. That is, all products start with a 3-year warranty and add 1 additional year for a total of 4 years; and 2 additional years for a total of 5 years.

the failed equipment (CONUS and OCONUS). In the event a same serial number component requested by the User cannot be repaired, the Contractor shall notify the Government User no later than three workdays after receipt of the component at the Contractor's facility. The Government User will provide the Contractor with disposition instructions for un-repairable pRFID components.

10.3 COMPONENT RETURN AND TRACKING

The Contractor shall provide a method to enable the Government User and the Contractor to quickly identify and track pRFID components that have been sent to a Contractor RC for warranty service. The Contractor shall assign a RMA number and inform the User of the RMA number as the tracking number, and serial number for each pRFID component returned to the Contractor for warranty service.

10.4 WARRANTY REPLACEMENT PARTS

The requirement for Contractor Warranty service is that only new parts, or parts warranted as new by the OEM, shall be used for repairs of failed Government pRFID components. Additionally, all replacement parts shall be equal to or better than the replaced parts in terms of quality and performance. The warranty for all replacement items installed during the initial warranty period shall be equal to the remaining warranty period for the original item, or 90 calendar days, whichever is greater. Failed parts replaced by the Contractor shall become the property of the Contractor. However, the Government reserves the right to purchase unserviceable parts containing sensitive or classified material, as required by statute or regulation.

10.5 WARRANTY ON-CALL PROCEDURES

The Contractor shall provide on-call warranty service for pRFID Fixed Readers in both CONUS and OCONUS. The requirement for CONUS locations is that the Contractor shall provide on-call repair no later than five workdays of notification. The requirement for OCONUS locations is that the Contractor shall provide on-call repair no later than seven workdays of notification. The Contractor shall provide on-call warranty service outside the official hours of operation when required by the using activity. When warranty service outside the official hours of operation are ordered in CONUS locations, the Contractor shall replace or return the equipment to an operational condition no later than five calendar days from the time the Contractor is notified of the malfunction. The requirement for OCONUS locations is that the Contractor shall replace or return the equipment to operational condition no later than seven calendar days of notification. The Contractor shall provide On-call Warranty service support to repair the item on-site.

11 MAINTENANCE

Upon expiration of the warranty, the Contractor shall provide worldwide maintenance to repair or replace pRFID components and provide updates and changes to software covered under maintenance. Maintenance prices shall include all parts, labor, and transportation back to the User.

11.1 MAINTENANCE TURN-AROUND TIME

The repaired pRFID component shall be returned and received by the User no later than ten workdays after receipt at the Contractor's facility. In the event the pRFID component cannot be repaired, the Contractor shall notify the Government User no later than three workdays after receipt of the component at the Contractor's facility. The Government User will provide the Contractor with disposition instructions for un-repairable RFID components.

11.1.1 pRFID Component Return and Tracking

The Contractor shall provide a method to enable the Government User and the Contractor to quickly identify and track pRFID components sent to a Contractor RC for Maintenance. The Contractor shall

assign a RMA number and inform the User of the RMA number as the tracking number and serial number for each pRFID component returned.

11.1.2 Mail-In Maintenance

The Contractor shall provide Mail-in Maintenance to include parts and labor on a Monthly and Per-incident basis for pRFID Fixed Readers, HHRs, and Printers. In accordance with Transportation paragraph in this section, the Contractor shall be responsible for transportation back to the User for all mail-in items.

11.1.3 On-Call Maintenance

The Contractor shall provide worldwide On-call Maintenance for pRFID Fixed Readers, HHRs and Printers. When maintenance service is ordered in CONUS locations, the Contractor shall replace or return the equipment to an operational condition no later than five workdays from the time the Contractor is notified of the malfunction. The requirement for OCONUS locations is that the Contractor shall replace or return the equipment to operational condition no later than seven workdays of notification.

The Contractor shall provide on-call maintenance outside the official hours of operation when required by the using activity. When maintenance outside the official hours of operation is ordered for CONUS locations, the Contractor shall replace or return the equipment to an operational condition no later than three workday's days from the time the Contractor is notified of a failure. When maintenance outside the official hours of operation is ordered for OCONUS locations, the Contractor shall replace or return the equipment to operational condition no later than five calendar days of notification. The Contractor shall provide the required maintenance service in accordance with the TO issued for the instant requirement or in accordance with a TO issued pursuant to the subparagraph entitled "Special Funding of Per Incident Maintenance" in Section I.

11.1.4 Maintenance Procedures

The Contractor shall replace or return equipment to an operational condition and ship the equipment back to the User no later than ten workdays after receipt of the failed equipment (CONUS and OCONUS). Transportation arrangements shall be in accordance with the provisions of the paragraph entitled "Transportation" in this Part. In the event a pRFID component cannot be repaired or if any discrepancy is noted between the equipment received and the TO, the Contractor shall notify the Government User no later than three workdays after receipt of the component at the Contractor's facility. The Government User will provide the Contractor with disposition instructions for un-repairable pRFID components.

11.1.5 Maintenance Replacement Parts

Contractor Maintenance support shall utilize only new parts, or parts warranted as new by the OEM, that shall be used for repairs of failed Government pRFID components. Additionally, all replacement parts shall be equal to or better than the replaced parts in terms of quality and performance. Failed parts replaced by the Contractor shall become the property of the Contractor. However, the Government reserves the right to purchase unserviceable parts containing sensitive or classified material, as required by statute or regulation to be destroyed or retained by the Government. The effective warranty for all replacement items installed during the maintenance period shall be a minimum of 90 calendar days.

11.1.6 Software Maintenance

The Contractor shall provide Software maintenance for all commercial software provided under this Contract in accordance with customary commercial software maintenance terms and conditions offered to the public to include all fixes, updates and changes necessary to maintain the software in an operational state. Software maintenance releases and software updates shall support all developed applications (fielded

or not) that are developed under the TES portion of the contract. Such support shall include, but is not limited to Application Interfaces and firmware changes.

11.2 PREVENTIVE MAINTENANCE

Preventive maintenance includes all actions performed in an attempt to retain an item in a specified condition by providing systematic inspection, detection, and prevention of incipient failures. Unless otherwise specified, Government personnel will perform all preventive maintenance for items acquired under this Contract. The Contractor shall provide to the Government, in detail, all requirements and procedures for preventive maintenance and troubleshooting-level diagnostics, in documentation and User Manuals. The Contractor shall provide Material Safety Data Sheets (MSDS) to the KO, COR and all users as specified in the individual order in accordance with FAR Clause 52.223-3 in Section I. The Contractor shall provide documentation for each appropriate hardware CLIN that shall include preventive maintenance checks, service schedules, and troubleshooting-level diagnostics. The Contractor shall be responsible for all other maintenance and support.

11.3 TRANSPORTATION

Transportation of pRFID components shipped to the Contractor for Maintenance will be arranged and paid for by the Government. Return transportation of repaired or replaced components shipped to the User shall be arranged and paid for by the Contractor. The Contractor shall use a return shipping method equal to or better than the User's method of shipment to the Contractor. The Government will provide the Contractor with any unusual transportation instructions for return shipment after repair.

12 TECHNICAL ENGINEERING SERVICES

12.1 GENERAL

The Contractor shall provide TES on-site at Government sites and at the Contractor's facility as specified in the TO. TES shall include those services required for End to End, RFID turnkey implementation, IUID implementation support, equipment integration, site analysis, installation, de-installation, relocation, problem-solving, user unique training, IPT support, conducting PCAs/FCAs, software development; communications, interfaces to other Government systems, post implementation maintenance, equipment and systems engineering services, System Design and systems integration to include middleware integration to enterprise systems. Any cables or adapters not listed in this Contract, middleware or other items and materials required for installation of Contractor-provided pRFID components, may be ordered through this Contract in accordance with the provision entitled "Incidental Materials". TES shall be ordered by a TO only. The Contractor shall maximize the use of hardware on the most recent pRFID contract whenever possible. All hardware and software solutions require Government approval. Contractor shall identify any requirements for interface with any other systems and identify required data elements as well as the digital requirements for implementation of the End-to-End Turn-key solution. The Government Program Manager will have the right to reject or require correction of any deficiencies found in the system, subsystem, or supply items that do not meet the requirements of the TES. Government rights under DFARS 227.7203-5(a) applies to all contractor developed software which is delivered for turnkey solutions via TES.

12.1.1 Proposal Request for TES

The Government will issue proposal requests for TES in accordance with Government Contracting Officer's Ordering Guide, paragraphs *Ordering Procedures for Orders Exceeding \$3,000*, and *Task Order – Technical Engineering Services*. The Contractor is encouraged to respond to all proposal requests by the specified submission dates. Proposals submitted in response to a proposal request shall comply with the requirements of the Government Contracting Officer's Ordering Guide.

12.1.2 Travel

Prices for Contractor personnel travel and per diem to perform TES shall be in accordance with the requirements set forth in “Task Orders – Technical Engineering Services”.

12.1.3 TES Trip Report

The Contractor shall submit a TES Trip Report to the TO POC or TO COR, if applicable, no later than five workdays after the completion of each trip made for TES. The trip report shall be in the Contractor’s format and shall contain as a minimum:

Report Date;

- a. Customer Name, address, POC and telephone number;
- b. Project Name;
- c. Time arrived, time departed;
- d. Any recommended or provided Incidental Material description;
- e. Contractor’s summary of work completed;
- f. Contractor POC name and signature.

12.1.4 TES Response Time

The Contractor shall provide TES within the time specified in the TO for specific technical services. The on-site locations and objectives of the TES to be provided shall be stated in the TO.

12.1.5 Software Development Services

Software Development Services (SDS) shall be limited to development incidental to the pRFID-related mission that utilizes equipment acquired under this Contract. The pRFID SDS shall be limited to the development work required to implement, modify, interface, and integrate pRFID application(s) to an existing Government application(s) and database(s) (e.g., SARSS, TIS). Services include new software development, which may include translation of existing Government code that has been determined necessary to ensure operation of the system.

12.2 INSTALLATION / DE-INSTALLATION / RELOCATION

12.2.1 Site Surveys and Installation Plans

The Contractor shall conduct a pre-installation, de-installation, or relocation site survey as specified in the TO for each location requiring site survey services. The primary purpose of the site survey is to determine the scope of work for the required installation, de-installation or relocation of pRFID equipment configurations. Within ten workdays after completion of the site survey, the Contractor shall provide an Installation Plan with supporting documentation and attachments. The Contractor shall submit the Installation Plan via electronic mail to the point of contract specified in the TO. Individual documents of over 5 Megabytes in size may be provided by link to a web page or data repository for electronic download, provided they are individually listed and linked from within the original electronic mail message. The Installation Plan shall include, but is not limited to, the following items:

- a. Specific details on the methodology for installation and the resources required;
- b. Detailed description, by major subheadings, of all installation work to be done by the Contractor at the site, and scheduling and dependency of the various tasks;
- c. Site layout plan including detailed drawings or digital pictures of all components, such as racks, cabinets, or consoles;
- d. General component specifications including equipment, physical specifications, templates, manufacturer’s specific machine configuration and space requirements, special operational line-of-sight requirements between various components, lighting requirements, site construction requirements, power requirements, cabling requirements, network connections, communication lines, cooling requirements, shipping requirements, and all special requirements that do not fall under normal operating conditions;

- e. Description of any actions, such as site modifications, which the Government will complete prior to installation of the pRFID equipment, in sufficient detail to facilitate successful installation of the equipment.

12.2.2 Installation/De-installation

The Contractor shall install and de-install pRFID configurations as specified in the TO. The Contractor shall provide all necessary installation support equipment, cables for the interface of the various components forming an installation, including the pRFID devices, servers, peripheral devices, and power sources as required. Upon receipt of a TO requiring installation/de-installation, and in accordance with the schedule contained therein, the Contractor shall install/de-install pRFID equipment in accordance with the approved Installation Plan. In instances where work to be performed by the Contractor requires interaction with existing facilities and equipment, the Contractor shall be responsible for any damage to existing facilities or equipment. After installation is completed, the Contractor shall remove all packing, shipping, and storage materials left over from the installation.

12.2.3 Relocation of Passive RFID Components

Upon receipt of a TO requiring relocation of pRFID equipment, and in accordance with the schedule contained therein, the Contractor shall install pRFID equipment in accordance with the approved Installation Plan. The extent of the services performed by the Contractor shall be specified in the TO and may vary from minimal involvement to total responsibility for the relocation.

12.2.4 Installation Plans

The Contractor shall submit an Installation Plan with supporting documentation and attachments for evaluation as a part of its proposal for TES. The Installation Plan shall include, but is not limited to, the following items:

- a. Specific details of the methodology for the installation and the resources required;
- b. Detailed description, by major subheadings, of all installation work to be accomplished by the Contractor at the site to include scheduling and dependency of the various tasks;
- c. Site layout plan including detailed drawings of all pRFID components, such as racks, cabinets, or consoles;
- d. General component specifications including equipment, physical specifications, templates, manufacturer's specific machine configuration and space requirements, special operational line-of-sight requirements between various components, lighting requirements, site construction requirements, power requirements, cabling requirements, network connections, communication lines including satellite communications, cooling requirements, shipping requirements, and all special requirements that do not fall under normal operating conditions;
- e. Description of any actions, such as site modifications, which the Government will complete prior to installation of the pRFID equipment, in sufficient detail to facilitate successful installation of the equipment.

12.3 CONTRACT SUPPORT PERSONNEL.

The Contractor shall provide all technical labor categories described in Attachment 0003 Labor Categories Descriptions. The Government will issue proposal requests for specific tasks to be performed under TOs. Personnel performing TES and training under this Contract shall possess the qualifications that the Contractor requires for, and be part of the same work force, providing such services to the public. The Contractor shall provide labor categories that represent a blend of demonstrated technical, supervisory and managerial expertise, analytical skills and knowledge to provide specific tasks, using efficient and state-of-the-art processes, made up of functions including, but not limited to, the following:

- a. pRFID component integration;
- b. Installation and de-installation;
- c. User unique training, on-site or classroom;
- d. Systems integration;
- e. Complex programming support;
- f. Designing, developing, and troubleshooting complex applications;
- g. Modeling simulation;
- h. Analysis in designing operating systems utilities;
- i. Troubleshooting, following established testing procedures to ensure equipment is operating properly;
- j. Development and revision of technical documentation for software, hardware, and systems;
- k. Testing online documents for correct operation, content and usability;
- l. Analyzing systems to identify project objectives and data elements;
- m. Preparing high level flow-charts and diagrams from which detailed program designs may be further developed;
- n. Database management, associated data analysis and design, and data dictionary tools, as well as distributed systems, and data base development methods and techniques;
- o. Total system development and integration efforts, including all equipment, software, telecommunications, and networks, based on expert knowledge of automatic identification and data capture fields;
- p. Outlining problems, and providing solutions to data communication projects and problems based on expert knowledge of modern data transfer methods and networks;
- q. Technical problem analysis and resolution based on expert knowledge of RF equipment and systems, wireless technologies, and wireless test procedures requirement analysis.

13 DOCUMENTATION REQUIREMENTS

13.1 GOVERNMENT RIGHTS

The Government shall have full and unrestricted rights, in accordance with copyright laws and regulations, to use and reproduce for its own use, all documentation provided under this Contract as described in and governed by DFARS 227.7202-1(a). The Contractor shall provide the RFID user community with online access to, including the capability to download, all User Manuals and software reference documentation for any piece of equipment that interfaces with a host computer system. User Manuals and software documentation shall be in English and in the Contractor's format using Portable Document Format (PDF) files.

13.2 COMMERCIAL USER MANUALS

The Contractor shall provide commercial User Manuals for each piece of equipment that provide step-by-step procedures for each function performed by the equipment. These User manuals shall identify all preventive maintenance tasks and troubleshooting procedures. The commercial User Manuals shall be included with each delivered piece of equipment and shall not be separately priced.

13.3 SOFTWARE REFERENCE DOCUMENTATION

The Contractor shall provide software reference documentation for use by software developers creating Passive RFID applications for all software offered in hard copy and for online access. The documentation shall contain specific details for the integration of pRFID equipment. The documentation shall be at a level of detail sufficient to fully define the operator interface and application operations. The software reference documentation shall be included with each delivered piece of equipment and shall not be separately priced.

14 TRAINING REQUIREMENTS

14.1 WEB BASED AND CD-ROM TRAINING

The Contractor shall provide multimedia training as specified herein. Training shall be provided on CD-ROM and via the internet on a trusted web site. The Web Based training shall allow users to train from the web site and have the ability to download a version of the training for execution on a standalone windows based computer. The training shall instruct the students how to operate, maintain, and repair the equipment, and develop unique application software programs for pRFID equipment acquired under this Contract. The Contractor shall provide a web-based and CD-ROM training package with updates for the base period of the Contract. Training updates may include the addition of new or modified products and other types of training updates as necessary.

14.1.1 Target Audiences and Areas

Target audiences utilizing the pRFID training will include technically skilled specialists responsible for supporting and implementing the use of pRFID components and end Users responsible for operating the Contractor-provided hardware and software. The pRFID Configuration Training shall encompass an overview of instruction in the following areas:

- a. pRFID Configuration Overview (hardware, software, communications). Hardware characteristics and principles of operation, pRFID Configuration hierarchy and software components (including the Operating System communication software interfaces), data structures, queues, and internal tables of the Operating System;
- b. Hardware and Software Architecture. Communications processing (including protocols), software designs, interfaces, and assembly (Operating System development) language.
- c. Operating System commands;
- d. Operating System tailoring and generation, method for the distribution of fixes, problem resolution, and implementation of new software releases;
- e. Operations of equipment to include, but not limited to: configuring Reader(s), collecting information, reading and writing information, searching data to identify priorities and finding specific items, creating prioritized lists of containers to be unloaded, and locating specific containers based on container number or content data;
- f. Diagnostics to include, but not limited to: problem definition and resolution, and diagnostic software utilization;
- g. Security features (including management considerations, controls, procedures, and software design); and
- h. Hardware maintenance and support. Preventive maintenance checks and services, and user-level repair operations.

14.1.2 Training

The Contractor shall provide access to Web Based training materials showing user installation instructions, start-up, or and downloads for diagnostics or software updates. The contractor shall provide a CD-ROM with the same materials offered on the Web with the initial shipment of each device as user documentation and Training materials; or provide a help/tutorial application on the device (not mandatory). At a minimum, the government desires materials cover topics such as hardware and software installation, problem diagnostics, performance measurements, diagnostic software, and basic component operations.

14.1.3 Special Training Materials

Under Technical Engineering Services, the government may order and the Contractor shall provide PD AMIS with Multi-media training materials. Such requests may include requirements for a draft storyboard(s) and draft graphical materials no later than 60 calendar days after the date of the first TO for the Web-Based or CD-ROM training. PD AMIS will review and approve the drafts and provide comments

to the Contractor. The Contractor shall amend or edit the draft MMTP based on the Government's comments and resubmit a revised draft no later than 14 calendar days after receipt of the Government's comments. The Contractor shall provide the final MMTP no later than 30 calendar days after receipt of PD AMIS's final approval of the draft MMTP materials. The Contractor shall at the Government's discretion attend a minimum of two meetings at PD AMIS designated facilities to provide for Government review and input into the MMTP prior to PD AMIS final approval of the draft MMTP materials. The Contractor shall provide PD AMIS draft storyboards, scripts, and graphics materials ten workdays prior to each meeting. The Contractor shall also provide an agenda at least ten workdays prior to each meeting, and shall provide meeting minutes no later than ten workdays after the conclusion of each meeting.

14.1.4 Training Deliverables

If ordered, the Contractor shall provide the following items in accordance with the approved MMTP within 45 days after approval of the MMTP or within 45 days after the date of the order, whichever is later:

- a. Web-based training
- b. One (1) Master CD-ROM to be used by the Government for reproduction and distribution purposes. This Master CD-ROM, along with a one (1) copy of the CD-ROM, shall be delivered to the COR.

14.1.5 Training Package Updates

Prior to implementing updates to the training package, the Contractor shall submit the updates to the COR for approval.

15 CERTIFICATION

15.1 PASSIVE RFID CERTIFICATIONS

15.1.1 Energy Star

Equipment meeting the specifications defined in PB 95-250304 shall be certified by the Contractor and properly labeled as meeting the Environmental Protection Agency (EPA) requirements.

15.1.2 NI Certification

The Contractor shall certify that equipment identified as NI, as well as its sub-components, shall be designed, manufactured and tested to NI standards, as specified at time of order in the most current NEC, for the environment specified in the paragraph 3.3.3 "Hazardous Environment."

15.1.3 Product Safety Certification

Equipment shall be certified that it meets ANSI/UL1950-1997. Such certification shall be made by an authorized, Nationally Recognized Testing Laboratory.

15.1.4 Electromagnetic Compatibility (EMC) Compliance and Hazards of Electromagnetic Radiation to Ordnance (HERO) Compliance

All applicable equipment shall meet, as appropriate, the requirements of National Telecommunications and Information Administration (NTIA) Manual Annex K, FCC Part 15, regulations for Government operations and, International Standards. In order to certify the use of commercial Passive RFID equipment in these environments, the Government may subject representative categories of equipment to radiated emission and susceptibility tests (See MIL-STD 461E: Requirements for the Control of Electromagnetic Interference

Emissions and Susceptibility, and MIL-STD-462E: Measurement of Electromagnetic Interference Characteristics). The applicable equipment shall remain unchanged after installation of Contractor-provided internal devices. All applicable equipment for CONUS shall meet the International Special Committee on Radio Interference (CISPR) 22, Class A (International) standards for Radio Frequency Interference/Electromagnetic Interference, and be Underwriters and European Community certified. .

15.1.5 Self-Certification.

The Contractor's self-certification of standards (e.g., ISO 9075) and DISR shall be based on the results of testing or inspection the Contractor undertakes or authorizes others to undertake on the Contractor's behalf. Self-certification shall be performed in accordance with ANSI Z-34.2-1987, American National Standards Institute (ANSI) for Certification — Self-Certification by Producer or Supplier.

16 BACKGROUND INVESTIGATIONS FOR CONTRACTOR PERSONNEL

16.1 BACKGROUND

When applicable, Contractor personnel performing services under this contract, TO shall be required to undergo a background investigation. TOs may require Contractor personnel to have access to Unclassified Sensitive information in accordance with DoDD 8500.01E, DoDI 8500.2, AR-25, and the Privacy Act of 1974 (Public Law 93-579). At a minimum, some CONUS and OCONUS TOs will require the Contractor personnel accessing this information to have a favorable National Agency Check (NAC) and/or a DoD Secret clearance (Interim Secret clearances are acceptable). Investigative packages may contain the following forms:

1. SF-85, Questionnaire for Non-Sensitive Positions
2. SF-85P, Questionnaire for Public Trust Positions
3. SF-86, Questionnaire for National Security Positions
4. Credit Report Release Form
5. FD-258, Fingerprint Card,

16.2 NAC FILE RECORDS

- a. The Contractor shall take the necessary steps to ensure the ability to timely respond to the TOs stating a requirement for a NAC or DoD Secret clearance. When a TO specifically addresses a requirement for a NAC, the Contractor personnel assigned to this effort shall complete a Standard Form 85 or 85P. When a TO specifically addresses a requirement for a DoD Secret clearance, the Contractor personnel assigned to this effort shall complete a Standard Form 86.
- b. The completed paperwork shall be submitted to the Contractor Security Manager for review of completeness. The Contractor Security Manager shall obtain a DoD Secret clearance from the Defense Security Service (DSS) or from the appropriate Government agency. The Contractor shall maintain a record of all requested NAC and DoD Secret clearance approvals and disapprovals.

16.3 CONTINUED PERFORMANCE DURING SUPPORT OF CRISIS SITUATIONS, CONTINGENCY OR EXERCISE

The Contractor shall provide continued performance during support of crisis situations, contingency or exercise in accordance with the paragraph entitled "Continued Performance During Support of Crisis Situations, Contingency or Exercise" in Government Contracting Officer's Ordering Guide.

17 ORGANIZATION CONFLICT OF INTEREST (OCI).

17.1 NON-DISCLOSURE AGREEMENT

- a. Due to the nature of the work to be performed under this contract the contractor may be required to submit signed non-disclosure agreement forms for all personnel working on a specific delivery/TO under this contract. Individual delivery/TOs will detail the scope of work to be performed under this contract. Without exception, all contractors are required to report potential OCI issues to the KO immediately regardless of the stage of the acquisition/contract/order (e.g., Pre-solicitation, pre-award, post award) and regardless of what provisions and clauses are provided for in the contract/order. The cognizant KO will provide the specific certificate of non-disclosure when applicable.
- b. Organizational Conflicts of Interest (OCI): Per FAR 9.5, OCI may result when factors create an actual or potential conflict of interest on a contract, or when the nature of the work to be performed on the contract creates an actual or potential conflict of interest on a future acquisition. In this procurement, the Army has particular concerns that any proposal received from an Offeror which would have the potential to perform services on any implementation contract to which that Offeror is organizationally connected, is likely to result in an impermissible "Impaired Objectivity", "Unequal Access to Information" or "Biased Ground Rules" OCI (one or more), and thus be ineligible for award under FAR 9.5. Therefore, with respect to this Contract and subsequent TOs, the contractor agrees that, in consideration of the award of this contract, the contractor, any subcontractor, consultant, or employee of the contractor, any joint venture involving the contractor, any entity with which it is or becomes affiliated by common ownership or with or into which it merges, or any successor or assignee of the contractor, shall not provide services as a prime, subcontractor or consultant under any systems integrator contract for current or future Army PEO EIS programs. The contractor shall include this requirement in subcontracts at all tiers. The contractor agrees that this restraint shall extend throughout this contract/TO period of performance, including any exercised options. The contractor agrees and acknowledges that compliance with this restraint at all tiers is a material requirement of this TO and the contract. (FAR 9.505-1) The only exception to these restrictions will be if the contractor submits a comprehensive mitigation plan to the KO that, at the sole discretion of the KO, gives the Government confidence that any current or potential OCIs will be satisfactorily neutralized.
- c. The Contractor agrees that if it assists in the preparation of non-developmental specifications or of work statements for a system or services under this Contract, or assists in the development of acquisition strategies or evaluation criteria or otherwise provides acquisition support under this Contract, it will not be allowed to furnish these items or services, either as a prime Contractor, a subcontractor or as a consultant (FAR 9.505-2).
- d. The Contractor agrees that if it gains access to proprietary data of other companies, it will protect such data, and it will not use such proprietary data in supplying systems or components in future competitive procurements (FAR 9.505-4). In addition, the Contractor agrees to protect the proprietary data and rights of other organizations disclosed to the Contractor during performance of this Contract with the same caution that a reasonably prudent Contractor would use to safeguard highly valuable property. The Contractor also agrees that if it gains access to the proprietary information of other companies that it will enter into an agreement with the other companies to protect their information from unauthorized use or disclosure for as long as it remains proprietary and refrain from using the information for any purpose other than that for which it was furnished.
- e. The Contractor agrees that it will not distribute reports, data or information of any nature arising from its performance under this Contract, except as provided by this Contract or as may be directed by the KO.
- f. The Contractor agrees that it will neither evaluate nor advise the Government with regard to its own products or activities. The Contractor will objectively evaluate or advise the Government concerning products or activities of any prospective competitors.

- g. The Contractor agrees that it will include the above provisions, including this paragraph, in agreements with teaming partners, consultants or subcontractors at any tier, which involve access to information covered above. The use of this Section 18 in such agreements shall be read by substituting the word "teaming partner," "consultant," or "subcontractor" for the word "Contractor" whenever the latter appears.
- h. Personal Conflicts of Interest: In the course of performance pursuant to this contract, Contractor employees will be participating personally and substantially in duties that have a direct and predictable effect upon other non-Federal entities. The Contractor agrees to use its best efforts to ensure those employees and others performing services under this contract avoid conflicts of interest or the appearance thereof. To that end, the Contractor agrees that its employees and others performing services under this contract will, prior to the commencement of performance, sign the Certificate of No Conflict of Interest provided by the cognizant KO.
- i. Personal and Substantial: To participate personally means to participate directly. It includes the direct and active supervision of the participation of a subordinate in the matter. To participate substantially means that the employee's involvement is of significance to the matter. Participation may be substantial even though it is not determinative of the outcome of a particular matter. However, it requires more than official responsibility, knowledge, perfunctory involvement, or involvement on an administrative or peripheral issue. A finding of substantiality should be based not only on the effort devoted to a matter, but also on the importance of the effort. While a series of peripheral involvements may be insubstantial, the single act of approving or participating in a critical step may be substantial. Personal and substantial participation may occur when, for example, an employee participates through decision, approval, disapproval, recommendation, investigation or the rendering of advice in a particular matter.
- j. Non-Disclosure. In the course of performance pursuant to this Contract, the Contractor will access nonpublic information, including acquisition sensitive information. The Contractor agrees that it will not use or disclose any such information unless authorized by the COR. Contractor further agrees that it will use its best efforts to ensure that its employees and others performing services under this Contract will not use or disclose any such information unless authorized by the COR. To that end, the Contractor agrees that its employees and others performing duties under this Contract will, prior to the commencement of performance, sign the Certificate of Non-Disclosure provided by the cognizant KO.

17.2 CATEGORIES OF CONFLICTING INTEREST

The following information is provided for clarity pertaining to the general OCI situations where conflicts may arise. OCI categories include, but are not limited to the following:

- a. Unequal Access to Information: A contractor has access to nonpublic information as part of its performance under a contract that leads to an unfair advantage in the competition for a later contract. Example: A support contractor obtains source selection sensitive information relating to procurement and competes for that procurement.
- b. Biased Ground Rules: A contractor sets the ground rules for a future competition. Example: A contractor develops requirements (such as the PWS or SOW) then competes to provide products or services to satisfy those requirements, thus obtaining a competitive advantage.
- c. Impaired Objectivity: A firm is asked to perform tasks that require objectivity, but another role the firm plays casts doubt on the firm's ability to be truly objective. Example: Where a contractor's work under a contract entails evaluating itself, a subsidiary or affiliate, or a competitor.

EXHIBIT- A

SAFE SEPARATION DISTANCE BETWEEN AN RF SOURCE AND UNSHIELDED MUNITIONS CONTAINING 10 mA NO-FIRE CURRENT ELECTRO-EXPLOSIVE DEVICES (EEDs)

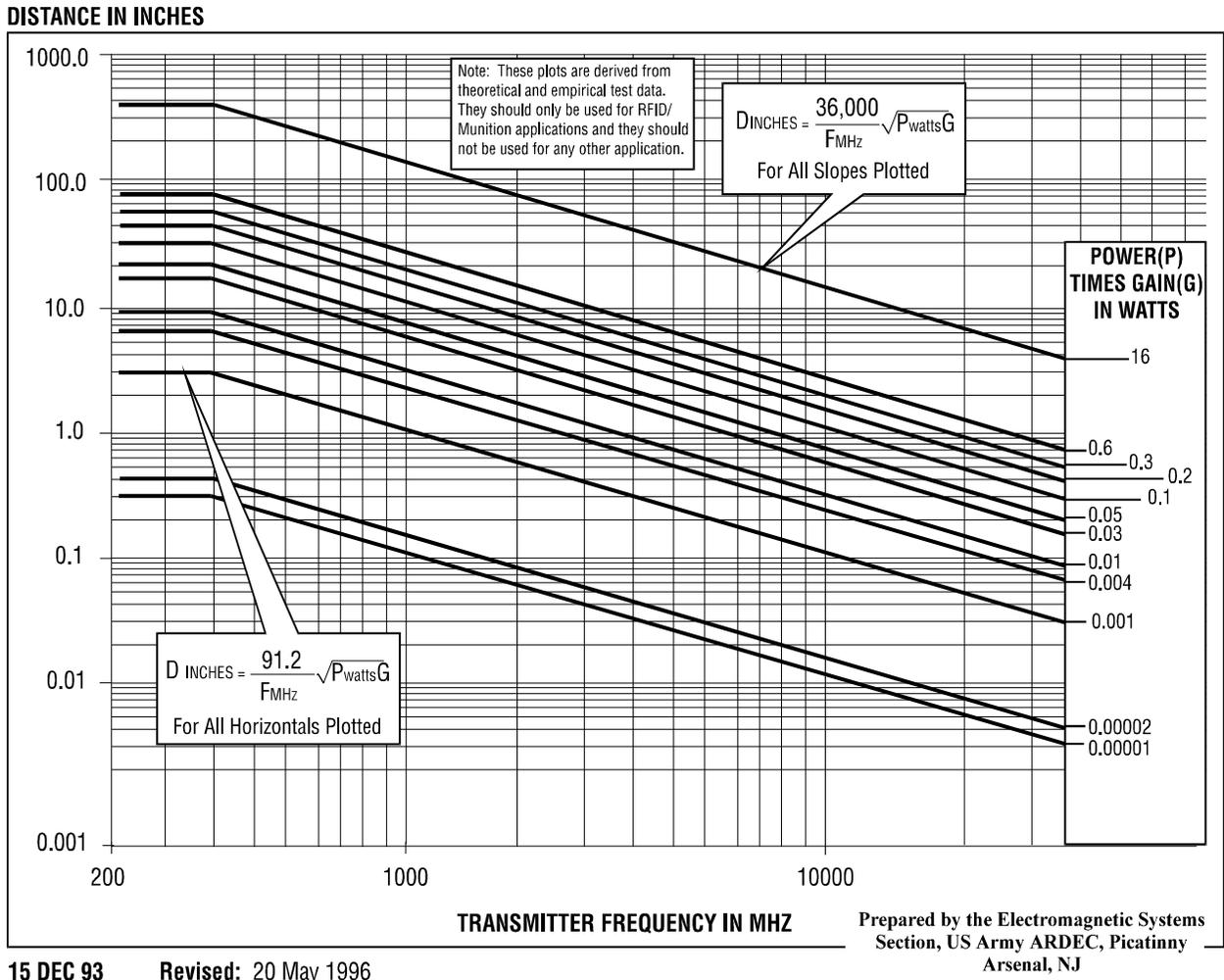


EXHIBIT-B

pRFID II Contract Status Report

CLIN	Description	Service	Month-Year		Year-to-Date		Contract-to-Date	
			Quantity	Total Amt	Quantity	Total Amt	Quantity	Total Amt
0001AA	pRFID Fixed Reader							
		Army	5	\$5	10	\$10	30	\$30
		AF	1	\$1	3	\$3	30	\$30
		Navy	10	\$10	30	\$30	50	\$50
		Marine	0	\$0	5	\$5	10	\$10
		Coast Guard	0	\$0	5	\$5	10	\$10
		DLA/Other	4	\$4	5	\$5	10	\$10
	TOTALS		20	\$20	58	\$58	140	\$140
0002BA	4" Wide Resin Ribbon							
		Army	10	\$50	20	\$100	50	\$250
		AF	0	\$0	3	\$15	10	\$50
		Navy	5	\$25	10	\$50	20	\$100
		Marine	0	\$0	0	\$0	2	\$10
		Coast Guard	0	\$0	0	\$0	0	\$0
		DLA/Other	0	\$0	5	\$25	10	\$50
	TOTALS		15	\$75	38	\$190	92	\$460

Contract Totals	Month-Year [Month / Year]		Year-to-Date [YEAR]		Contract-to-Date	
	Product	Services	Product	Services	Product	Services
Army	\$100	\$500	\$21,000	\$103,000	\$25,090	\$130,000
AF	\$0	\$0	\$3,000	\$0	\$3,000	\$0
Navy	\$6,000	\$0	\$6,000	\$0	\$6,000	\$0
Marine	\$0	\$0	\$12,000	\$85,000	\$12,000	\$85,000
Coast Guard	\$0	\$0	\$0	\$0	\$0	\$0
DLA/Other	\$0	\$0	\$5,200	\$0	\$0	\$0
SUB TOTALS	\$6,100	\$500	\$47,200	\$188,000	\$46,090	\$215,000
TOTAL	\$6,600		\$235,200		\$261,090	

Note: The CLINs, Description, Quantity numbers and Total Amounts shown above are for illustrative purposes only. The Contractor may provide each of the three summaries (Current month, Year-to-date, and Contract-to-date) on separate worksheets of the same spreadsheet file. The Contract totals table should be reflected on a separate sheet on the spreadsheet file.

EXHIBIT C

Antiterrorism/Operations Security (AT/OPSEC) Requirements

1. AT Level I training. *This standard language is for contractor employees with an area of performance within an Army controlled installation, facility or area.* All contractor employees, to include subcontractor employees, requiring access Army installations, facilities and controlled access areas shall complete AT Level I awareness training within 14 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR or to the contracting officer, if a COR is not assigned, within 14 calendar days after completion of training by all employees and subcontractor personnel. AT level I awareness training is available at the following website: <http://jko.jten.mil>

2. Access and general protection/security policy and procedures. *This standard language is for contractor employees with an area of performance within Army controlled installation, facility, or area.* Contractor and all associated sub-contractors employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

2a. For contractors requiring Common Access Card (CAC). Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05. The contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of 6 months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personnel Management.

2b. For contractors that do not require CAC, but require access to a DoD facility or installation. Contractor and all associated sub-contractors employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (**Army Directive 2014-05/AR 190-13**), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

3. AT Awareness Training for Contractor Personnel Traveling Overseas. This standard language required US based contractor employees and associated sub-contractor employees to make available and to receive government provided area of responsibility (AOR) specific AT awareness training as directed by AR 525-13. Specific AOR training content is directed by the combatant commander with the unit ATO being the local point of contact.

4. iWATCH Training. *This standard language is for contractor employees with an area of performance within an Army controlled installation, facility or area.* The contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be

completed within 14 calendar days of contract award and within 14 calendar days of new employees commencing performance with the results reported to the COR NLT 14 calendar days after contract award.

5. Army Training Certification Tracking System (ATCTS) registration for contractor employees who require access to government information systems. All contractor employees with access to a government info system must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services, and must successfully complete the DOD Information Assurance Awareness prior to access to the IS and then annually thereafter.

6. For contracts that require a formal OPSEC program. The contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer. This plan will include a process to identify critical information, where it is located, who is responsible for it, how to protect it and why it needs to be protected. The contractor shall implement OPSEC measures as ordered by the commander. In addition, the contractor shall have an identified certified Level II OPSEC coordinator per AR 530-1.

7. For contracts that require OPSEC Training. Per AR 530-1 *Operations Security*, the contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter.

8. For information assurance (IA)/information technology (IT) training. All contractor employees and associated sub-contractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M and AR 25-2 within six months of appointment to IA/IT functions.

9. For information assurance (IA)/information technology (IT) certification. Per DoD 8570.01-M , DFARS 252.239.7001 and AR 25-2, the contractor employees supporting IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award.

10. For contractors authorized to accompany the force. DFARS Clause 252.225-7040, *Contractor Personnel Authorized to Accompany U.S. Armed Forces Deployed Outside the United States*. The clause shall be used in solicitations and contracts that authorize contractor personnel to accompany US Armed Forces deployed outside the US in contingency operations; humanitarian or peacekeeping operations; or other military operations or exercises, when designated by the combatant commander. The clause discusses the following AT/OPSEC related topics: required compliance with laws and regulations, pre-deployment requirements, required training (per combatant command guidance), and personnel data required

11. For Contract Requiring Performance or Delivery in a Foreign Country, DFARS Clause 252.225-7043, *Antiterrorism/Force Protection for Defense Contractors Outside the US*. The clause shall be used in solicitations and contracts that require performance or delivery in a foreign country. This clause applies to both contingencies and non-contingency support. The key AT requirement is for non-local national contractor personnel to comply with theater clearance requirements and allows the combatant commander to exercise oversight to ensure the contractor's compliance with combatant commander and subordinate task force commander policies and directives.

12. For contracts that require handling or access to classified information. Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with— (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); (2) any revisions to DOD 5220.22-M, notice of which has been furnished to the contractor.

13. Threat Awareness Reporting Program. For all contractors with security clearances. Per AR 381-12 Threat Awareness and Reporting Program (TARP), contractor employees must receive annual TARP training by a CI agent or other trainer as specified in AR 381-12, para 2-4b.