

CONTRACT NNL06AA05B

(Contract)

The following information has been determined to be exempt from disclosure and has been deleted from the contract:

- Exhibit D – Subcontracting Plan
- Exhibit E – “Messaging Servers Standard” portion of IT Security Plan

The Subcontracting Plan is replete with proprietary information and because there are no reasonably segregable portions that are subject to release, this plan is being withheld in its entirety.

The deleted material is exempt from disclosure under 14 C.F.R. 1206.300(b)(4) which covers trade secrets and commercial or financial information obtained from a person and privileged and confidential information. It has been held that commercial or financial material is “confidential” for purposes of this exemption if its disclosure would be likely to have either of the following effects: (1) impair the Government’s ability to obtain necessary information in the future; or (2) cause substantial harm to the competitive position of the person from whom the information was obtained, *National Parks and Conservation v. Morton*, 498 F2d 765 (D.C. Cir. 1974). Certain portions of Exhibit E - IT System Security Plan for NASA Technology Transfer System have also been determined to be exempt from disclosure and have been deleted under FOIA Exemption 2, which exempts from mandatory disclosure records that are "related solely to the internal personnel rules and practices of an agency. Computer Security Plans that all federal agencies are required by law to prepare may be withheld under FOIA Exemption 2 to prevent unauthorized access to information which could result in altercation, loss, damage or destruction of data contained in a computer system.

AWARD/CONTRACT	1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 350)	RATING C-9	PAGE 1 of 40 + Exhibits
2. CONTRACT NO. NNL06AA05B	3. EFFECTIVE DATE See Block 20 C. Below	4. REQUISITION/PURCHASE REQUEST/PROJECT NO. See Block 14. Below	

5. ISSUED BY NASA Langley Research Center 9B Langley Boulevard Hampton, VA 23681-2199	CODE	6. ADMINISTERED BY (If other than Item 5) C. Lynn Jenkins, Contracting Officer Mail Stop 126 Phone: 757-864-3284 Fax: 757-864-7709 Email: Lynn.Jenkins@nasa.gov
--	------	---

7. NAME AND ADDRESS OF CONTRACTOR (No., street, city, country, State and ZIP Code) Honeywell Laboratories 3660 Technology Drive Minneapolis, MN 55418 Name: Dan Retka Phone: 612-951-7854 Email: dan.retka@honeywell.com Fax: 612-951-7595	Cage Code: 27327 TIN: 22-2640650	8. DELIVERY <input type="checkbox"/> FOB ORIGIN <input checked="" type="checkbox"/> FOB Destination
		9. DISCOUNT FOR PROMPT PAYMENT Net 30
		10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN

CODE:	FACILITY CODE	IN: > ITEM Contract Para. G2
-------	---------------	------------------------------

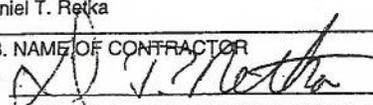
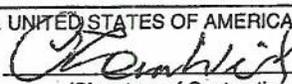
11. SHIP TO/MARK FOR CODE	12. PAYMENT WILL BE MADE BY MS 175/Comm Acctg Section NASA Langley Research Center Hampton, VA 23681-2199
------------------------------	--

13. AUTHORITY FOR USING OTHER THAN FULL & OPEN COMPETITION: <input checked="" type="checkbox"/> 10 U.S.C. 2304(c) (1) <input checked="" type="checkbox"/> 41 U.S.C. 253(c) (1)	14. ACCOUNTING AND APPROPRIATION DATA 4200139726 \$25,000 (Complete)
---	---

15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
1	TITLE: "Flight Critical Systems Research (FCSR)" 5-Year IDIQ Task Order Contract.	1	EA	See Contract Para. B.2	See Contract Para. B.2
15G. TOTAL AMOUNT OF CONTRACT >					See B.2

16. TABLE OF CONTENTS							
(X)	.SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES			
<input checked="" type="checkbox"/>	A	SOLICITATION/CONTRACT FORM	1	<input checked="" type="checkbox"/>	I	CONTRACT CLAUSES	28
<input checked="" type="checkbox"/>	B	SUPPLIES OR SERVICES AND PRICES/COSTS	2	PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.			
<input checked="" type="checkbox"/>	C	DESCRIPTION/SPECS./WORK STATEMENT	3	<input checked="" type="checkbox"/>	J	LIST OF ATTACHMENTS	40
<input checked="" type="checkbox"/>	D	PACKAGING AND MARKING	7	PART IV - REPRESENTATIONS AND INSTRUCTIONS			
<input checked="" type="checkbox"/>	E	INSPECTION AND ACCEPTANCE	8	<input type="checkbox"/>	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
<input checked="" type="checkbox"/>	F	DELIVERIES OR PERFORMANCE	9	<input type="checkbox"/>	L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
<input checked="" type="checkbox"/>	G	CONTRACT ADMINISTRATION DATA	10	<input type="checkbox"/>	M	EVALUATION FACTORS FOR AWARD	
<input checked="" type="checkbox"/>	H	SPECIAL CONTRACT REQUIREMENTS	14				

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

17. <input checked="" type="checkbox"/> CONTRACTOR'S NEGOTIATED AGREEMENT (Contractor is required to sign this document and return 1 copies to issuing office.) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (attachments are listed herein.)	18. <input type="checkbox"/> AWARD (Contractor is not required to sign this document.) Your offer on Solicitation Number _____, including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the items listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your offer, and (b) this award/contract. No further contractual document is necessary.
19A. NAME AND TITLE OF SIGNER (Type or print) Daniel T. Retka	20A. NAME OF CONTRACTING OFFICER (Type or print) C. Tom Weih
19B. NAME OF CONTRACTOR BY  (Signature of person authorized to sign)	20B. UNITED STATES OF AMERICA BY  (Signature of Contracting Officer)
19C. DATE SIGNED 1/12/2006	20C. DATE SIGNED 1/13/06

PART I - THE SCHEDULE

SECTION B - SUPPLIES OR SERVICES AND PRICE/COSTS

B.1 SUPPLIES AND/OR SERVICES TO BE FURNISHED

Except as may be expressly stated in the task orders as furnished by the Government, the Contractor shall provide all resources as specified in Task Orders issued pursuant to Clause H.8, Task Ordering Procedure, that are necessary to perform the requirements delineated in the Section C, Statement of Work.

B.2 MINIMUM AND MAXIMUM INDEFINITE DELIVERY, INDEFINITE QUANTITY (IDIQ) CONTRACT VALUE

The guaranteed minimum quantity of work which will be required under this contract, and which will be initiated through the issuance of task orders, shall be **\$25,000**. There will be no further obligation on the part of the Government to issue additional task orders thereafter. The total maximum aggregate value is **\$35 million** for the 5-year period of performance (total of all multiple award contracts).

B.3 ESTIMATED COST AND FIXED FEE

The estimated cost and fixed fee of the contract is the sum of the estimated costs and fixed fee set forth for individual Task Orders issued by the Government pursuant to H.8, Task Ordering Procedure.

B.4 CONTRACT FUNDING (NFS 18-52.232-81) (JUN 1990)

- (a) Contract funding will be provided at the task order level.
- (b) The Limitation of Funds Clause FAR 52.232-22 (APR 1984) applies at the Task Order level.

SECTION C - DESCRIPTION/SPECIFICATION/WORK STATEMENT

Flight Critical Systems Research

1.0 Background/Introduction

The NASA Langley Research Center Research and Technology Directorate Airborne Systems focus area mission is to develop useable research and technology tools, methods, and techniques, which enable the delivery of future airborne systems technologies for the NASA Aeronautics and Exploration Systems Mission Directorates. This statement of work (SOW) defines the requirements for Flight Critical Systems Research to assist NASA in fulfilling this mission, and will evolve as the Agency's mission evolves. Flight Critical Systems Research addresses avionics systems technology gaps that are exposed by the operational challenges of the future national airspace system, trans-atmospheric flight, and extra-terrestrial planetary flight. Such operations are characterized by increasing complexity/integration; distributed control; onboard diagnostics and prognostics; un-crewed vehicle operations and autonomy; blurring of system boundaries; ubiquitous automation/computing; and increasing verification, validation, and certification challenges.

2.0 Scope

The Contractor shall conduct basic and applied research, technology development, systems analyses, and systems integration in avionics systems critical to flight management and control. The work to be performed will be defined in performance based Task Orders issued by the Contracting Officer in accordance with Section H, H.8 TASK ORDERING PROCEDURE (NFS 1852.216-80) (October 1996). The Contractor shall be responsible for defining operational and system requirements, and for delivering engineering and research results that meet the specific technical requirements defined in the SOW of each Task Order. The Contractor shall furnish all personnel, facilities, equipment, material, supplies, and services to perform the work as outlined in each Task Order, with the exception of items designated as Government furnished. The general Work Areas to be performed under the Task Orders are outlined below.

3.0 Flight Dynamics, Guidance, and Control

This Work Area includes, but is not limited to: attached and separated-flow aerodynamics; static and dynamic stability; control effector characteristics; dynamic modeling methods; flight-control-law effects; flying and handling qualities; agility and maneuverability; out-of-control flight characteristics; guidance and control theory; control system concepts; controls allocation/ reconfiguration; and control law design. Specific research topics include, but are not limited to, development of technologies, which enhance the ability of the flight crew to respond correctly when critical system or component failures occur; prevent related occurrences of loss of control in flight; enable automated responses to mitigate loss of control; and reduce the pilot workload associated with maintaining safe flight. This work area also includes the modeling and simulation associated with Flight Dynamics, Guidance, and Control research and development.

3.1 The Contractor shall develop guidance and control technologies for operation throughout the flight envelope to (1) prevent loss of vehicle control, and (2) recover vehicle control from loss-of-control (upset) conditions resulting from adverse flight conditions and vehicle/system failures, occurring separately or in combinations.

3.2 The Contractor shall consider and evaluate the following adverse conditions, including, but not limited to: external disturbances; atmospheric disturbances (e.g. wake vortices); weather (e.g. wind shear, turbulence, icing); internal errors; crew input errors (e.g. mode confusion, pilot induced oscillations); system errors/malfunctions (e.g. software/hardware, HIRF [High Intensity Radiated Fields]); external interference; aircraft; and terrain/fixed obstacles.

3.3 The Contractor shall consider and evaluate the following vehicle and system failures, including, but not limited to: control system component failures; sensors; actuators; propulsion system; vehicle impairment and damage; control surface impairment and damage; and fuselage and lifting body impairment and damage. Consideration shall be given to coupling effects between flight control, structure, and propulsion system damage.

3.4 The Contractor shall consider and evaluate the following vehicle upset conditions, including, but not limited to: operation beyond the normal vehicle flight envelope; unstable modes of motion; stall and/or departure from controlled flight; uncommanded motions due to asymmetric thrust or failures; and out-of-control motions (e.g., falling leaf).

3.5 The Contractor shall consider and evaluate the integration of vehicle health management and guidance and control functions, with emphasis on, but not limited to the following issues: definition and utilization of diagnostic information for control performance effectiveness assessment and; definition and utilization of prognostic information for predicting and averting loss of control conditions and for life extending control.

3.6 The Contractor shall develop guidance and control technologies, investigate flight dynamics, and develop simulation concepts and methods related to multi-vehicle scenarios. Such scenarios include, but are not limited to, formation flight.

4.0 Crew Systems and Aviation Operations

This Work Area includes, but is not limited to: integrated flight deck systems; aircraft self-separation and distributed air traffic management; atmospheric hazard awareness and avoidance; situation awareness assessment; synthetic vision; and human-centered design. These research areas investigate aviation safety and airspace capacity issues such as controlled flight into terrain (CFIT), loss of control in flight, runway incursions, and high density air traffic operations.

4.1 The Contractor shall develop technologies and methods that provide real-time information electronically, to flight crews to improve their situation awareness. Types of real-time information include, but are not limited to: current position in four dimensional space; traffic locations and identity; terrain and obstacle locations; hazardous weather location and type; flight path or surface route information; air traffic control (ATC) instructions; and alerts of impending/potential hazardous situations. The Contractor shall investigate and evaluate display concepts that reduce uncertainties associated with real-time information presentation.

4.2 The Contractor shall develop communication, navigation, and surveillance infrastructure technologies required to acquire, process, and disseminate situation awareness information.

4.3 The Contractor shall develop technologies and methods aimed at increasing the situation awareness of air traffic controllers, including, but not limited to: systems to enable both strategic and tactical collaborative decision making; seamless surveillance; controller-pilot datalink communications (CPDLC); and alerting of path/route deviations by flight crews.

4.4 The Contractor shall investigate and develop technologies, methods and procedures to enable high density operations in the future airspace system. Elements and functions of such operations shall include, but not be limited to: air and ground-based traffic management; all-weather operations; terrain-impacted navigation; and detection and accommodation of wake turbulence.

4.5 The Contractor shall complete all documentation and meet all requirements to conduct experimentation with human subjects, in accordance with NASA Procedural Requirement 7100.1 "Protection of Human Research Subjects" (available at the NASA Online Directives Information System <http://nodis.hq.nasa.gov/>) and the NASA Langley Research Center Institutional Review Board (IRB).

5.0 Reliable and Robust Avionics Systems

This Work Area includes, but is not limited to: mathematical proof of safety properties for software and hardware; quantitative analysis to ensure functionality, reliability, and safety; fault tolerance; fault modeling and emulation; real-time upset detection and recovery; architecture concepts to improve system robustness to disturbances; vehicle health management; commercial-off-the-shelf technology in safety-critical systems; complexity modeling and management; and integrated modular avionics. Specific research topics include, but are not limited to: the prevention and reduction of malfunctions and failures in aircraft systems and components by developing design and assessment tools to verify system design correctness and validate required system functionality; and the investigation, development, and integration of existing and future sensing/processing technologies to enable vehicle-wide health monitoring.

5.1 The Contractor shall develop and demonstrate methods, techniques, and tools for the design, verification, integration, validation, and certification of complex and highly integrated mission and life critical systems. Highly integrated, complex systems are composed of functionally and physically different entities that must operate in seamless and safe coordination. Such entities include, but are not limited to, mechanical, electrical, computational, and human components. The Contractor shall develop methods, techniques, and tools to guarantee that the following systems criteria are met: safety; required performance; design correctness; immunity to disturbances in electromagnetic environments (EME); information integrity and security in presence of malicious and environmental threats; and fault containment, recovery, and accommodation.

5.2 The Contractor shall investigate methods that quantify the system's ability to perform to specification in the presence of faults.

5.3 The Contractor shall develop databases from analytical, simulation, and flight investigations of flight critical systems' performance in failure/damage situations. Such databases shall be capable of providing the basis for new system designs and for new assessment techniques and tools.

5.4 The Contractor shall develop concepts, methods, and technologies for distributed, onboard health diagnostic and prognostic system architectures and algorithms. The Contractor shall validate new health monitoring and diagnostic/prognostic system concepts in the context of catastrophic failure prevention and mitigation, and decreased maintenance costs as it applies to major vehicle systems, including, but not limited to:

5.4.1 Malfunctions and failures of the aircraft propulsion system, such as engine surge, asymmetric thrust, and turbomachinery crack/fatigue growth and propagation.

5.4.2 Damage of the airframe (including the wings, fuselage, and control surface attachment points), such as crack/fatigue growth and propagation, and/or damage resulting from malicious threats.

5.4.3 Anticipated and unanticipated malfunctions and failures of the aircraft flight systems (including the electrical power generation/distribution system; digital computers for guidance, navigation, control, and flight management; crew station computers, displays, cueing, warning, and annunciation systems; the digital data bus; sensors; and control actuation components), such as functional error modes in computers, bus errors, short circuits, blocked Pitot tubes, and faulty sensors and actuators.

5.4.4 Providing crew members with the possible consequences of systems failures, the symptom and indicators of such consequences, and correct crew responses to mitigate consequences.

5.4.5 Providing onboard capability to utilize prognostic data to adapt control strategies that delay the onset of failures and utilize diagnostic data to mitigate failures when they occur.

6.0 Flight Critical Systems Analysis and Integration

This work area includes, but is not limited to, performance of systems engineering in support of novel flight critical systems analysis and development from research concept through simulation and test to flight experiment.

6.1 The Contractor shall conduct the following: requirements analysis; complex system functional decomposition; experimental system specification; experimental system design; system verification and validation; cost-benefit studies; modeling and simulation; configuration management; systems integration; and systems assurance. The Contractor shall perform all analyses and develop all documentation necessary to obtain cognizant safety authority approval as determined by the LaRC Airworthiness and Safety Review Board (ASRB). This includes experimental flight system(s) flown on NASA aircraft, or Contractor-owned and university-owned aircraft funded by NASA.

SECTION D - PACKAGING AND MARKING

D.1 LISTING OF CLAUSES INCORPORATED BY REFERENCE

NOTICE: The following contract clauses pertinent to this section are hereby incorporated by reference:

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1)

CLAUSE NUMBER	DATE	TITLE
------------------	------	-------

None included by reference.

II. NASA FAR SUPPLEMENT (48 CFR CHAPTER 18) CLAUSES

CLAUSE NUMBER	DATE	TITLE
------------------	------	-------

None included by reference.

SECTION E - INSPECTION AND ACCEPTANCE

E.1 LISTING OF CLAUSES INCORPORATED BY REFERENCE

NOTICE: The following contract clauses pertinent to this section are hereby incorporated by reference:

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1)

CLAUSE NUMBER	DATE	TITLE
52.246-9	APR 1984	INSPECTION OF RESEARCH AND DEVELOPMENT (SHORT FORM)

II. NASA FAR SUPPLEMENT (48 CFR CHAPTER 18) CLAUSES

CLAUSE NUMBER	DATE	TITLE
------------------	------	-------

None included by reference.

E.2 HUMAN SPACE FLIGHT ITEM (NASA 1852.246-73) (MARCH 1997)

The Contractor shall include the following statement in all subcontracts and purchase orders placed by it in support of this contract, without exception as to amount or subcontract level:

"FOR USE IN HUMAN SPACE FLIGHT; MATERIALS, MANUFACTURING, AND WORKMANSHIP OF HIGHEST QUALITY STANDARDS ARE ESSENTIAL TO ASTRONAUT SAFETY.

IF YOU ARE ABLE TO SUPPLY THE DESIRED ITEM WITH A HIGHER QUALITY THAN THAT OF THE ITEMS SPECIFIED OR PROPOSED, YOU ARE REQUESTED TO BRING THIS FACT TO THE IMMEDIATE ATTENTION OF THE PURCHASER."

SECTION F - DELIVERIES OR PERFORMANCE

F.1 LISTING OF CLAUSES INCORPORATED BY REFERENCE

NOTICE: The following contract clauses pertinent to this section are hereby incorporated by reference:

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1)

CLAUSE NUMBER	DATE	TITLE
52.211-15	SEP 1990	DEFENSE PRIORITY AND ALLOCATION REQUIREMENTS
52.242-15	AUG 1989	STOP-WORK ORDER (ALTERNATE I) (APR 1984)
52.247-34	NOV 1991	F.O.B. DESTINATION

II. NASA FAR SUPPLEMENT (48 CFR CHAPTER 18) CLAUSES

CLAUSE NUMBER	DATE	TITLE
------------------	------	-------

None included by reference.

F.2 PERIOD OF PERFORMANCE (LaRC 52.211-91) (NOV 2002)

The period for issuance of task orders is 60 months from the effective date of this contract.

F.3 DELIVERY REQUIREMENTS (LaRC 52.211-96) (APR 2002)

Delivery shall be f.o.b. destination:

National Aeronautics and Space Administration
Langley Research Center
4 South Marvin Street (Bldg. 1206)
Hampton VA 23681-2199

or as specified in each task order.

F.4 PLACE(S) OF PERFORMANCE (LaRC 52.211-98) (OCT 1992)

The place(s) of performance shall be:

The Contractor's facility located in Minneapolis, MN or Phoenix, AZ and other sites as may be specified by task orders.

SECTION G - CONTRACT ADMINISTRATION DATA

G.1 LISTING OF CLAUSES INCORPORATED BY REFERENCE

NOTICE: The following contract clauses pertinent to this section are hereby incorporated by reference:

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1)

CLAUSE NUMBER	DATE	TITLE
------------------	------	-------

None included by reference.

II. NASA FAR SUPPLEMENT (48 CFR CHAPTER 18) CLAUSES

CLAUSE NUMBER	DATE	TITLE
1852.216-75	DEC 1988	PAYMENT OF FIXED FEE
1852.242-73	NOV 2004	NASA CONTRACTOR FINANCIAL MANAGEMENT REPORTING
1852.245-70	JUL 1997	CONTRACTOR REQUESTS FOR GOVERNMENT-OWNED EQUIPMENT

G.2 SUBMISSION OF VOUCHERS FOR PAYMENT (NFS 1852.216-87) (MAR 1998)

(a) The designated billing office for cost vouchers for purposes of the Prompt Payment clause of this contract is indicated below. Public vouchers for payment of costs shall include a reference to the number of this contract.

(b) (1) If the Contractor is authorized to submit interim cost vouchers directly to the NASA paying office, the original voucher should be submitted to:

NASA Langley Research Center
MS 175/ Accounts Payable
Hampton VA 23681

(2) For any period that the Defense Contract Audit Agency has authorized the Contractor to submit interim cost vouchers directly to the Government paying office, interim vouchers are not required to be sent to the Auditor, and are considered to be provisionally approved for payment, subject to final audit.

(3) Copies of vouchers should be submitted as directed by the Contracting Officer.

(c) If the Contractor is not authorized to submit interim cost vouchers directly to the paying office as described in paragraph (b), the Contractor shall prepare and submit vouchers as follows:

(1) One original Standard Form (SF) 1034, SF 1035, or equivalent Contractor's attachment to the Contractor's DCAA office.

(2) Three copies of SF 1034, SF 1035A, or equivalent Contractor's attachment to the following offices by insertion in the memorandum block of their names and addresses:

(i) Copy 1 NASA Contracting Officer

(ii) Copy 2 Auditor

(iii) The Contracting Officer may designate other recipients as required.

(d) (1) Public vouchers for payment of fee shall be prepared similarly to the procedures in paragraphs (b) or (c) of this clause, whichever is applicable, and be forwarded to:

NASA Langley Research Center
MS 175 / Accounts Payable
Hampton VA 23681

This is the designated billing office for fee vouchers for purposes of the Prompt Payment clause of this contract.

(2) Fixed fee shall be paid in monthly installments based upon the percentage of completion of work as determined by the Contracting Officer. The following formulas are provided as a convenience for calculating the interim fee provided the formulas produce a reasonable percentage as compared to completion of work. You should show both formulas on your fee voucher, however, the maximum fee percentage for fee billing is the smaller of the percentages resulting from the application of the two formulas. If at any time the Contracting Officer determines that the fee percentage is not consistent with the completion of work, the fee formula will be adjusted, or another methodology that results in comparative fee billing agree upon.

(#) $\frac{\text{Cost Incurred to Date}}{\text{Contract Estimated Cost}} = \%$

(#) $\frac{\text{Months of Performance Expended to Date}}{\text{Contract Period of Performance (Months)}} = \%$

(e) In the event that amounts are withheld from payment in accordance with provisions of this contract, a separate voucher for the amount withheld will be required before payment for that amount may be made.

G.3 DESIGNATION OF NEW TECHNOLOGY REPRESENTATIVE AND PATENT REPRESENTATIVE (NASA 1852.227-72) (JUL 1997)

(a) For purposes of administration of the clause of this contract entitled "New Technology" or "Patent Rights -- Retention by the Contractor (Short Form)", whichever is included, the following named representatives are hereby designated by the Contracting Officer to administer such clause:

New Technology Representative
Office Code 141
NASA Langley Research Center
Hampton, VA 23681-2199

Patent Representative
Office Code 141
NASA Langley Research Center
Hampton, VA 23681-2199

(b) Reports of reportable items, and disclosure of subject inventions, interim reports, final reports, utilization reports, and other reports required by the clause, as well as any correspondence with respect to such matters, should be directed to the New Technology Representative unless transmitted in response to correspondence or request from the Patent Representative. Inquires or requests regarding disposition of rights, election of rights, or related matters should be directed to the Patent Representative. This clause shall be included in any subcontract hereunder requiring a "New Technology" clause or "Patent Rights--Retention by the Contractor (Short Form)" clause, unless otherwise authorized or directed by the Contracting Officer. The respective responsibilities and authorities of the above-named representatives are set forth in 1827.305-370 of the NASA FAR Supplement.

G.4 FINANCIAL REPORTING OF NASA PROPERTY IN THE CUSTODY OF CONTRACTORS (NFS 1852.245-73) (OCT 2003)

(a) The Contractor shall submit annually a NASA Form (NF) 1018, NASA Property in the Custody of Contractors, in accordance with the provisions of 1845.505-14, the instructions on the form, subpart 1845.71, and any supplemental instructions for the current reporting period issued by NASA.

(b) (1) Subcontractor use of NF 1018 is not required by this clause; however, the Contractor shall include data on property in the possession of subcontractors in the annual NF 1018.

(2) The Contractor shall mail the original signed NF 1018 directly to the cognizant NASA Center Deputy Chief Financial Officer, Finance, unless the Contractor uses the NF 1018 Electronic Submission System (NESS) for report preparation and submission.

(3) One copy shall be submitted (through the Department of Defense (DOD) Property Administrator if contract administration has been delegated to DOD) to the following address: [Insert name and address of appropriate NASA Center office.], unless the Contractor uses the NF 1018 Electronic Submission System (NESS) for report preparation and submission.

- (c) (1) The annual reporting period shall be from October 1 of each year through September 30 of the following year. The report shall be submitted in time to be received by October 15. The information contained in these reports is entered into the NASA accounting system to reflect current asset values for agency financial statement purposes. Therefore, it is essential that required reports be received no later than October 15. Some activity may be estimated for the month of September, if necessary, to ensure the NF 1018 is received when due. However, Contractor procedures must document the process for developing these estimates based on planned activity such as planned purchases or NASA Form 533 (NF 533 Contractor Financial Management Report) cost estimates. It should be supported and documented by historical experience or other corroborating evidence, and be retained in accordance with FAR Subpart 4.7, Contractor Records Retention. Contractors shall validate the reasonableness of the estimates and associated methodology by comparing them to the actual activity once that data is available, and adjust them accordingly. In addition, differences between the estimated cost and actual cost must be adjusted during the next reporting period. Contractors shall have formal policies and procedures, which address the validation of NF 1018 data, including data from subcontractors, and the identification and timely reporting of errors. The objective of this validation is to ensure that information reported is accurate and in compliance with the NASA FAR Supplement. If errors are discovered on NF 1018 after submission, the Contractor shall contact the cognizant NASA Center Industrial Property Officer (IPO) within 30 days after discovery of the error to discuss corrective action.
- (2) The Contracting Officer may, in NASA's interest, withhold payment until a reserve not exceeding \$25,000 or 5 percent of the amount of the contract, whichever is less, has been set aside, if the Contractor fails to submit annual NF 1018 reports in accordance with 1845.505-14 and any supplemental instructions for the current reporting period issued by NASA. Such reserve shall be withheld until the Contracting Officer has determined that NASA has received the required reports. The withholding of any amount or the subsequent payment thereof shall not be construed as a waiver of any Government right.
- (d) A final report shall be submitted within 30 days after disposition of all property subject to reporting when the contract performance period is complete in accordance with (b)(1) through (3) of this clause.

SECTION H - SPECIAL CONTRACT REQUIREMENTS

H.1 LISTING OF CLAUSES INCORPORATED BY REFERENCE

NOTICE: The following contract clauses pertinent to this section are hereby incorporated by reference:

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1)

CLAUSE NUMBER	DATE	TITLE
------------------	------	-------

None included by reference.

II. NASA FAR SUPPLEMENT (48 CFR CHAPTER 18) CLAUSES

CLAUSE NUMBER	DATE	TITLE
1852.208-81	NOV 2004	RESTRICTIONS ON PRINTING AND DUPLICATING
1852.223-70	APR 2002	SAFETY AND HEALTH
1852.223-74	NOV 2004	DRUG- AND ALCOHOL-FREE WORKFORCE
1852.223-75	FEB 2002	MAJOR BREACH OF SAFETY OR SECURITY
1852.242-78	APR 2001	EMERGENCY MEDICAL SERVICES AND EVACUATION
1852.244-70	APR 1985	GEOGRAPHIC PARTICIPATION IN THE AEROSPACE PROGRAM

H.2 SECURITY CLASSIFICATION REQUIREMENTS (NASA 1852.204-75) (SEP 1989)

Performance under this contract will involve access to and/or generation of classified information, work in a security area, or both, up to the level of Secret, as Determined in Individual Task Orders. See Federal Acquisition Regulation clause 52.204-2 in this contract and DD Form 254, Contract Security Classification Specification, Exhibit B.

H.3 SECURITY PROGRAM/NON-U.S. CITIZEN EMPLOYEE ACCESS REQUIREMENTS (LaRC 52.204-91) (OCT 2003)

(a) Access to the LaRC by contractor non-U.S. citizen employees, including employees in permanent resident alien status, shall be approved in accordance with NPG 1371.2 and LMS-CP-4850-- "Non-U.S. Citizen(s)/Foreign Representative(s) Visitor Approval". Administrative processing requires advance notice of between 20 to 45 days depending on the nationality of the non-U.S. citizen. Access authorization shall be for a maximum of one year, and must be reevaluated annually. Non-U.S. citizen employees must be under escort at all times while on Center by a U.S. citizen issued a LaRC identification badge.

(b) Request for Center access in excess of 90 days requires that a background investigation be conducted on the non-U.S. citizen employee. The processing of a background investigation requires the submittal of a NASA Form 531, "Name Check Request," and a fingerprint card application. Normal processing time for a background investigation is approximately 90 days. A favorably adjudicated background investigation shall allow non-U.S. citizen contractor employee limited unescorted access to the Center. Access shall be limited to work areas identified and deemed necessary and entry and egress to that site.

H.4 RELEASE OF SENSITIVE INFORMATION (NFS 1852.237-73) (JUNE 2005)

(a) As used in this clause, "sensitive information" refers to information, not currently in the public domain, that the Contractor has developed at private expense, that may embody trade secrets or commercial or financial information, and that may be sensitive or privileged.

(b) In accomplishing management activities and administrative functions, NASA relies heavily on the support of various service providers. To support NASA activities and functions, these service providers, as well as their subcontractors and their individual employees, may need access to sensitive information submitted by the Contractor under this contract. By submitting this proposal or performing this contract, the Contractor agrees that NASA may release to its service providers, their subcontractors, and their individual employees, sensitive information submitted during the course of this procurement, subject to the enumerated protections mandated by the clause at 1852.237-72, Access to Sensitive Information.

(c) (1) The Contractor shall identify any sensitive information submitted in support of this proposal or in performing this contract. For purposes of identifying sensitive information, the Contractor may, in addition to any other notice or legend otherwise required, use a notice similar to the following:

Mark the title page with the following legend:

This proposal or document includes sensitive information that NASA shall not disclose outside the Agency and its service providers that support management activities and administrative functions. To gain access to this sensitive information, a service provider's contract must contain the clause at NFS 1852.237-72, Access to Sensitive Information. Consistent with this clause, the service provider shall not duplicate, use, or disclose the information in whole or in part for any purpose other than to perform the services specified in its contract. This restriction does not limit the Government's right to use this information if it is obtained from another source without restriction. The information subject to this restriction is contained in pages [insert page numbers or other identification of pages].

Mark each page of sensitive information the Contractor wishes to restrict with the following legend:

Use or disclosure of sensitive information contained on this page is subject to the restriction on the title page of this proposal or document.

(2) The Contracting Officer shall evaluate the facts supporting any claim that particular information is "sensitive." This evaluation shall consider the time and resources necessary to protect the information in accordance with the detailed safeguards mandated by the clause at 1852.237-72, Access to Sensitive Information. However, unless the Contracting Officer decides, with the advice of Center counsel, that reasonable grounds exist to challenge the Contractor's claim that particular information is sensitive, NASA and its service providers and their employees shall comply with all of the safeguards contained in paragraph (d) of this clause.

(d) To receive access to sensitive information needed to assist NASA in accomplishing management activities and administrative functions, the service provider must be operating under a contract that contains the clause at 1852.237-72, Access to Sensitive Information. This clause obligates the service provider to do the following:

- (1) Comply with all specified procedures and obligations, including the Organizational Conflicts of Interest Avoidance Plan, which the contract has incorporated as a compliance document.
- (2) Utilize any sensitive information coming into its possession only for the purpose of performing the services specified in its contract.
- (3) Safeguard sensitive information coming into its possession from unauthorized use and disclosure.
- (4) Allow access to sensitive information only to those employees that need it to perform services under its contract.
- (5) Preclude access and disclosure of sensitive information to persons and entities outside of the service provider's organization.
- (6) Train employees who may require access to sensitive information about their obligations to utilize it only to perform the services specified in its contract and to safeguard it from unauthorized use and disclosure.
- (7) Obtain a written affirmation from each employee that he/she has received and will comply with training on the authorized uses and mandatory protections of sensitive information needed in performing this contract.
- (8) Administer a monitoring process to ensure that employees comply with all reasonable security procedures, report any breaches to the Contracting Officer, and implement any necessary corrective actions.

(e) When the service provider will have primary responsibility for operating an information technology system for NASA that contains sensitive information, the service provider's contract shall include the clause at 1852.204-76, Security Requirements for Unclassified Information Technology Resources. The Security Requirements clause requires the service provider to implement an Information Technology Security Plan to protect information processed, stored, or transmitted from unauthorized access, alteration, disclosure, or use. Service provider personnel requiring privileged access or limited privileged access to these information technology systems are subject to screening using the standard National Agency Check (NAC) forms appropriate to the level of risk for adverse impact to NASA missions. The Contracting Officer may allow the service provider to conduct its own screening, provided the service provider employs substantially equivalent screening procedures.

(f) This clause does not affect NASA's responsibilities under the Freedom of Information Act.

(g) The Contractor shall insert this clause, including this paragraph (g), suitably modified to reflect the relationship of the parties, in all subcontracts that may require the furnishing of sensitive information.

H.5 OBSERVATION OF REGULATIONS AND IDENTIFICATION OF CONTRACTOR'S EMPLOYEES (LaRC 52.211-104) (APR 2002)

(a) Observation of Regulations--In performance of that part of the contract work which may be performed at Langley Research Center or other Government installation, the Contractor shall require its employees to observe the rules and regulations as prescribed by the authorities at Langley Research Center or other installation including all applicable Federal, NASA and Langley safety, health, environmental and security regulations.

(b) Identification Badges--At all times while on LaRC property, the Contractor shall require its employees, Subcontractors and agents to wear badges which will be issued by the NASA LaRC Badge and Pass Office, located at 1 Langley Boulevard (Building No. 1228). Badges shall be issued only between the hours of 6:30 a.m. and 3:30 p.m., Monday through Friday. Contractors will be held accountable for these badges, and may be required to validate outstanding badges on an annual basis with the NASA LaRC Security Office. Immediately upon employee termination or contract completion, badges shall be returned to the NASA LaRC Badge and Pass Office. It is agreed and understood that all NASA identification badges remain the property of NASA and the Government reserves the right to invalidate such badges at any time.

(c) Employee Outprocessing--The Contractor shall ensure that all employees who are terminated or no longer connected with work being performed under this contract are out processed through the LaRC Badge and Pass Office. Badges and keys must be accounted for and returned.

H.6 INCORPORATION OF SECTION K OF THE PROPOSAL BY REFERENCE (LaRC 52.215-107) (NOV 2002)

Pursuant to FAR 15.204-1(b), the completed Section K of the proposal is hereby incorporated by reference.

H.7 Reserved**H.8 TASK ORDERING PROCEDURE (NFS 1852.216-80) (OCT 1996)**

(a) Only the Contracting Officer may issue task orders to the Contractor, providing specific authorization or direction to perform work within the scope of the contract and as specified in the schedule. The Contractor may incur costs under this contract in performance of task orders and task order modifications issued in accordance with this clause. No other costs are authorized unless otherwise specified in the contract or expressly authorized by the Contracting Officer.

(b) Prior to issuing a task order, the Contracting Officer shall provide the Contractor with the following data:

(1) A functional description of the work identifying the objectives or results desired from the contemplated task order.

(2) Proposed performance standards to be used as criteria for determining whether the work requirements have been met.

(3) A request for a task plan from the Contractor to include the technical approach, period of performance, appropriate cost information, and any other information required to determine the reasonableness of the Contractor's proposal.

(c) Within 14 calendar days after receipt of the Contracting Officer's request, the Contractor shall submit a task plan conforming to the request.

(d) After review and any necessary discussions, the Contracting Officer may issue a task order to the Contractor containing, as a minimum, the following:

- (1) Date of the order.
- (2) Contract number and order number.
- (3) Functional description of the work identifying the objectives or results desired from the task order, including special instructions or other information necessary for performance of the task.
- (4) Performance standards, and where appropriate, quality assurance standards.
- (5) Maximum dollar amount authorized (cost and fee or price). This includes allocation of award fee among award fee periods, if applicable.
- (6) Any other resources (travel, materials, equipment, facilities, etc.) authorized.
- (7) Delivery/performance schedule including start and end dates.
- (8) If contract funding is by individual task order, accounting and appropriation data.

(e) The Contractor shall provide acknowledgment of receipt to the Contracting Officer within 3 calendar days after receipt of the task order.

(f) If time constraints do not permit issuance of a fully defined task order in accordance with the procedures described in paragraphs (a) through (d), a task order which includes a ceiling price may be issued.

(g) The Contracting Officer may amend tasks in the same manner in which they were issued.

(h) In the event of a conflict between the requirements of the task order and the Contractor's approved task plan, the task order shall prevail.

H.9 TASK ORDER SOLICITATION AND SELECTION PROCEDURES (LaRC 52.216-97) (OCT 2004)

(a) Each Contractor will be given a fair opportunity to be considered for each order in accordance with FAR 16.505. This contract includes no requirement for the Contractor to submit a proposal for any individual task order. The costs of preparing proposals for individual task orders under the contract will not be an allowable direct charge to the contract. However, these costs may be an allowable cost to the normal bid and proposal indirect cost pursuant to FAR 31.205-18.

The contracting officer (CO) will consider past performance, quality of services and/or deliverables, final proposed cost/price or other factors the contracting officer believes are relevant.

Contractors need not be given an opportunity to be considered for a particular order in excess of \$2,500 under multiple Task Order contracts if the CO determines that-

1. The agency need for such supplies or services is of such urgency that providing such opportunity would result in unacceptable delays;
2. Only one such Contractor is capable of providing such supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized;

3. The order should be issued on a sole-source basis in the interest of economy and efficiency as a logical follow-on to an order already issued under the contract, provided that all Contractors were given a fair opportunity to be considered for the original order; or
4. It is necessary to place an order to satisfy a minimum guarantee.

(b) The CO need not contact each of the multiple award Contractors before selecting an order awardee if the contracting officer has information available to ensure that each multiple Contractor is provided a fair opportunity to be considered for each order.

(c) For those orders, which are competed among the multiple contract awardees, the CO will provide a solicitation to each Contractor and will request a proposal in accordance with H.8, Task Ordering Procedure. The solicitation will include a Statement of Work, specifications, or drawings; required delivery date, any special instructions or provisions, and any selection criteria to be used to award the Task Order which differs from that specified in H.8. Prior to awarding the Task Order, all awardees will be required to provide a task plan that may include the following: 1) technical approach, 2) implementation plan (including staffing, proposed facilities and Subcontractors), 3) estimated cost including breakouts of the estimated labor hours and all costs to perform the Task Order, and 4) proposed fee. As required by NASA FAR Supplement 1815.404-471-5(a), when FCCOM is included as an item of cost in the Contractor's proposal, a reduction in the profit/fee objective will be made in an amount equal to the amount of FCCOM allowed in accordance with FAR 31.205-10(a)(2) or 1 percent of the cost base, whichever is less. The level of detail in each Task Plan will be dependent on the complexity of the requirement. Upon selection of an awardee, the CO and Contracting Officer Technical Representative (COTR) will review the task plan and cost estimate to complete the work. The contracting officer will negotiate any necessary changes with the Contractor. The final cost estimate represents the baseline to be used for reporting in Columns 7b and 7d of NASA Form 533M (See Exhibit A).

(d) Orders may be issued by facsimile or electronic commerce methods.

(e) No protest is authorized in connection with this contract except for a protest on the grounds that the order increases the scope, period, or maximum value of the contract.

(f) In the case where only one award is made as a result of this solicitation or if the CO determines that the Task Order shall not be competed (based on criteria stated in Paragraph A above), the following Task Order initiation procedure apply:

1. The COTR will provide a Statement of Work, specifications, or drawings; required delivery date, any special instructions or provisions to the Contractor.
2. The Contractor will be required to provide a task plan, which shall include a discussion of their technical approach for performing the work and an estimated cost for the proposed Task Order in accordance with H.8, Task Ordering Procedure. The estimated cost shall include breakouts of the estimated labor hours and costs to perform the Task Order.
3. The CO and COTR will review the task plan and cost estimate to complete the work. The CO will negotiate necessary changes with the Contractor.
4. The final negotiated cost estimate shall represent the baseline to be used for reporting in Columns 7b and 7d of NASA Form 533M (See Exhibit A).

H.10 SMALL DISADVANTAGED BUSINESS PARTICIPATION--CONTRACT TARGETS (LaRC 52.219-91) (OCT 2002) (for offeror fill-in)

Fill-In: By offeror

(a) This clause does not apply to, and should not be completed by Small Disadvantaged Business (SDB) offerors unless the SDB offeror has waived the price adjustment evaluation adjustment [see Paragraph (c) of FAR clause 52.219-23].

(b) FAR 19.1202-4(a) requires that SDB participation targets be incorporated in the contract. Targets for this contract are as follows: (See Internet at <http://www.census.gov/epcd/www/naics.html> for Department of Commerce NAICS Industry Subsectors.)

	<u>Department of Commerce NAICS Industry Subsector</u>	<u>Dollar Target</u>	<u>Percent of Contract Value</u>
Year 1	541710 and 561510	\$502,272	8.9%
Year 2	541710 and 561510	\$521,893	9.2%
Year 3	541710 and 561510	\$542,302	9.6%
Year 4	541710 and 561510	\$563,540	9.9%
Year 5	541710 and 561510	\$585,608	10.3%
5 Year Total (includes allocable indirect mat'l)		\$2,979,812	10.5%

(c) FAR 19.1202-4(b) requires that SDB concerns that are specifically identified by the offeror be listed in the contract when the extent of the identification of such Subcontractors was part of the SDB evaluation subfactor. SDB concerns (Subcontractors) specifically identified by the offeror are as follows:

Name of Concern(s):

Scientific Systems Co., Inc. (SSCI); Metro Travel.

The Contractor shall notify the Contracting Officer of any substitutions of firms that are not SDB concerns.

(d) If the prime offeror is an SDB (including joint venture partners and team members) that has waived the price evaluation adjustment, the target for the work it intends to perform as a prime Contractor in authorized Department of Commerce NAICS Industry Subsectors is as follows:

	<u>Percent of Dollars</u>	<u>Contract Value</u>
Year 1	n/a	n/a
Year 2	n/a	n/a
Year 3	n/a	n/a
Year 4	n/a	n/a
Year 5	n/a	n/a

NOTE: Because of the nature of this contract (i.e., Task Order IDIQ), the Government will annually evaluate the Contractor's performance in meeting the SDB NAICS Industry Standard goals based on the percentages proposed by the contractor within this clause and not based on the proposed dollar target amounts.

H.11 FLIGHT TEST OPERATIONS AND SAFETY REPORT (FTOSR) INFORMATION (LaRC 52.223-91) (OCT 2004)

The Technical Point of Contact (POC) and/or COTR must submit a Flight Test Operations and Test and Safety Report (FTOSR) to the Airworthiness and Safety review Board (ASRB) for evaluation and approval in order to obtain a Flight Safety Release letter. The Contractor shall support the Technical Point of Contact (POC) and/or COTR to obtain this Flight Safety Release letter when work performed under this contract requires experiments to be flown on or involving aircraft (including balloon borne experiments/instruments) whose flights occur within the Earth's sensible atmosphere. Specifically such flights include full-scale aircraft or aircraft models, either manned or unmanned and either powered or un-powered. No flight test/flight experiment shall be conducted until a Flight Safety Release letter is obtained. This is applicable for aircraft that are either NASA, University or Contractor-owned. The Contractor shall develop the FTOSR or information required for the FTOSR. The Flight Safety Release letter is obtained by the Technical Point of Contact (POC) and/or COTR from the LaRC Airworthiness and Safety Review Board (ASRB) per the requirements of LMS-CP-5580 Airworthiness and Safety Review Board process, and in accordance with LAPD-1710.1 Langley Research Center Aviation Safety Policy and LPR 1710.16 Aviation Operations and Safety Manual. An outline for the FTOSR is provided below. If an item in the FTOSR does not apply, the item must be marked as such and a brief reason why it does not apply.

Flight Test Operations and Safety Report (FTOSR) Outline:

A. Cover Sheet w/ Approvals

B. Program/Project Overview:

1. Program Objectives & General Description
2. Program Management
3. Selected Aircraft
4. Proposed Aircraft Modifications & Design Criteria
5. Instrumentation Hardware/software & Flt Test
6. Data Measurement Requirements
7. Contractual Requirements
8. Other Involved Agencies
9. Summary of Supporting Research & Tests (includes minutes of design review activities)
10. Analytical
11. Wind Tunnel
12. Simulation
13. Ground Operating Systems Check out
14. Proposed Schedule Milestones

C. Flight Test Operations:

1. Location
2. Flight Tests Start Date
3. Number of Flights
4. Flight Frequency
5. Test Procedures (incl. maneuvers)
6. Support Requirements:
7. Support Organization & Responsibilities
8. Transportation to Test Location
9. Chase Aircraft
10. Photo/TV Coverage
11. Tracking
12. Radar
13. Optical

14. Beacon (incl. frequency)
15. Telemetry
16. Communications
17. Meteorological
18. Data
19. Real Time
20. Quick Look
21. Processed
22. Other Special Support Requirements

D. Safety:

1. System Safety Program Plan
2. Risk Assessment
3. Hazard Analysis
4. General Operational Restrictions & Conditions
5. Weather
6. Personal Equipment
7. Minimum On-board Equipment
8. Weight/Balance
9. Flight Test Envelope
10. Abort Procedures
11. Emergency Plans & Procedures
12. Configuration Control Responsibilities
13. Other

H.12 EXPORT LICENSES (NFS 1852.225-70) (FEB 2000)

(a) The Contractor shall comply with all U.S. export control laws and regulations, including the International Traffic in Arms Regulations (ITAR), 22 CFR Parts 120 through 130, and the Export Administration Regulations (EAR), 15 CFR Parts 730 through 799, in the performance of this contract. In the absence of available license exemptions/exceptions, the Contractor shall be responsible for obtaining the appropriate licenses or other approvals, if required, for exports of hardware, technical data, and software, or for the provision of technical assistance.

(b) The Contractor shall be responsible for obtaining export licenses, if required, before utilizing foreign persons in the performance of this contract, including instances where the work is to be performed on-site at NASA Langley Research Center, where the foreign person will have access to export-controlled technical data or software.

(c) The Contractor shall be responsible for all regulatory record keeping requirements associated with the use of licenses and license exemptions/exceptions.

(d) The Contractor shall be responsible for ensuring that the provisions of this clause apply to its Subcontractors.

H.13 LaRC 52.227-28 HANDLING OF DATA (MAY 2003)

(a) "DATA," as used in this clause, means recorded information, regardless of the form, the media on which it may be recorded, or the method of recording. The term includes, but is not limited to, models, photographs, lab notebooks, diagrams, drawings, information subject to the Privacy Act, information of a scientific or technical nature, computer software and documentation thereof, and information of a commercial or financial nature.

(b) In the performance of this contract the Contractor will have access to, be furnished, generate, or use one or more of the following categories of DATA:

- (1) DATA of third parties that the Government has agreed to handle under protective arrangements;
- (2) Government DATA, the use and dissemination of which the Government intends to control or is required to control by law; or
- (3) DATA that the Contractor will create or assist in creating under this contract that the Government has agreed to handle under protective arrangements or indicates that it intends to control.

(c) In order to protect the interests of the Government and the owners, licensors and licensees of such DATA, the Contractor agrees, with respect to any of the types of DATA identified in paragraph (b), above, that is either marked with a restrictive legend, specifically identified to the Contractor as DATA being generated and to be marked with a restrictive legend, or otherwise identified in writing by the Contracting Officer or his or her representative as being subject to this clause, to:

- (1) Use, disclose, and reproduce such DATA only to the extent necessary to perform the work required under this contract;
- (2) Allow access to such DATA only to those of its employees that require access for their performance under this contract;
- (3) Preclude access and disclosure of such DATA by the Contractor's personnel outside of that portion of the Contractor's organization needed for the performance of the Contractor's duties under this contract; and
- (4) Return or dispose of such DATA, as the Contracting Officer or his or her representative may direct when the DATA is no longer needed for contract performance.

(d) In the event that DATA includes a legend that the Contractor deems to be ambiguous or unauthorized, the Contractor shall inform the Contracting Officer of such condition. Notwithstanding the ambiguous or unauthorized nature of such a legend, as long as the legend provides an indication that a restriction on the use or disclosure was intended, the Contractor shall treat such DATA pursuant to the requirements of this clause unless otherwise directed, in writing, by the Contracting Officer.

(e) Subject to the notice requirements in (f), below, the Contractor shall not be restricted in the use, disclosure, and reproduction of DATA that:

- (1) Is, or becomes, generally available or public knowledge without breach of this clause by the Contractor or its employees;
- (2) Is known to the Contractor at the time of disclosure; has been disclosed to the Contractor without restriction from the Government; or has been independently developed by the Contractor outside of the Contractor's activities under this contract;
- (3) Has become known to the Contractor without similar restrictions from a source other than the Government or any party having work performed under this contract, that source having the right to disclose such DATA; or
- (4) The Contractor is required to produce such DATA pursuant to a court order or similar Government action.

(f) If the Contractor believes that any event or condition removes the restrictions on their use, disclosure, or reproduction of DATA, the Contractor shall promptly notify the Contracting Officer in writing of such belief before acting on such belief, and, in any event, shall give written notice to the Contracting Officer before unrestricted use, disclosure, or reproduction of such DATA.

(g) Before the Contractor has access to DATA identified in paragraph (b), above, the Contractor shall provide the Contracting Officer an acceptable written plan by which it intends to assure that its personnel who have or might reasonably have access to any such DATA, will honor the Contractor's obligation to safeguard such DATA. Should the Contracting Officer consider the proposed plan inadequate, the Contractor will be advised of the inadequacy and the Contractor will provide a revised plan. The Contracting Officer may suspend work under this contract, at no cost to the Government, until such time as the written plan of the Contractor is considered acceptable to the Contracting Officer.

(h) The Contractor agrees to inform and instruct its employees of its and their obligations under this clause and to appropriately bind its employees contractually to comply with the access, use, disclosure, and reproduction provisions of this clause.

H.14 AIRCRAFT FLIGHT RISKS (NFS 1852.228-71) (DECEMBER 1988)

(a) Notwithstanding any other provision of this contract (particularly paragraph (g) of the Government Property (Cost-Reimbursement, Time-and-Materials, or Labor-Hour Contracts) clause and paragraph (c) of the Insurance--Liability to Third Persons clause), the Contractor shall not (1) be relieved of liability for damage to, or loss or destruction of, aircraft sustained during flight or (2) be reimbursed for liabilities to third persons for loss of or damage to property or for death or bodily injury caused by aircraft during flight, unless the flight crew members have previously been approved in writing by the Contracting Officer.

(b) For the purposes of this clause--

(1) Unless otherwise specifically provided in the Schedule, "aircraft" includes any aircraft, whether furnished by the Contractor under this contract (either before or after Government acceptance) or furnished by the Government to the Contractor under this contract, including all Government property placed or installed or attached to the aircraft, unless the aircraft and property are covered by a separate bailment agreement.

(2) "Flight" includes any flight demonstration, flight test, taxi test, or other flight made in the performance of this contract, or for the purpose of safeguarding the aircraft, or previously approved in writing by the Contracting Officer.

(i) With respect to land-based aircraft, flight commences with the taxi roll from a flight line and continues until the aircraft has completed the taxi roll to a flight line.

(ii) With respect to sea-planes, flight commences with the launching from a ramp and continues until the aircraft has completed its landing run and is beached at a ramp.

(iii) With respect to helicopters, flight commences upon engagement of the rotors for the purpose of take-off and continues until the aircraft has returned to the ground and rotors are disengaged.

(iv) With respect to vertical take-off aircraft, flight commences upon disengagement from any launching platform or device and continues until the aircraft has been re-engaged to any launching platform or device.

(3) "Flight crew members" means the pilot, copilot, and, unless otherwise specifically provided in the Schedule, the flight engineer and navigator when required or assigned to their respective crew positions to conduct any flight on behalf of the Contractor.

- (c) (1) If any aircraft is damaged, lost, or destroyed during flight and the amount of the damage, loss, or destruction exceeds \$100,000 or 20 percent of the estimated cost, exclusive of any fee, of this contract, whichever is less, and if the Contractor is not liable for the damage, loss, or destruction under the Government Property (Cost-Reimbursement, Time-and-Materials, or Labor-Hour Contracts) clause of this contract or under paragraph (a) of this clause, an equitable adjustment for any resulting repair, restoration, or replacement required under this contract shall be made (i) in the estimated cost, the delivery schedule, or both and (ii) in the amount of any fee to be paid to the Contractor, and the contract shall be modified in writing accordingly.
- (2) In determining the amount of adjustment in the fee that is equitable, any fault of the Contractor, its employees, or any Subcontractor that materially contributed to the damage, loss, or destruction shall be taken into consideration.

H.15 MINIMUM INSURANCE COVERAGE (NASA 1852.228-75) (OCT 1988)

The Contractor shall obtain and maintain insurance coverage as follows for the performance of this contract:

(a) Worker's compensation and employer's liability insurance as required by applicable Federal and state workers' compensation and occupational disease statutes. If occupational diseases are not compensable under those statutes, they shall be covered under the employer's liability section of the insurance policy, except when contract operations are so commingled with the Contractor's commercial operations that it would not be practical. The employer's liability coverage shall be at least \$100,000, except in States with exclusive or monopolistic funds that do not permit workers' compensation to be written by private carriers.

(b) Comprehensive general (bodily injury) liability insurance of at least \$500,000 per occurrence.

(c) Motor vehicle liability insurance written on the comprehensive form of policy which provides for bodily injury and property damage liability covering the operation of all motor vehicles used in connection with performing the contract. Policies covering motor vehicles operated in the United States shall provide coverage of at least \$200,000 per person and \$500,000 per occurrence for bodily injury liability and \$20,000 per occurrence for property damage. The amount of liability coverage on other policies shall be commensurate with any legal requirements of the locality and sufficient to meet normal and customary claims.

(d) Comprehensive general and motor vehicle liability policies shall contain a provision worded as follows:

"The insurance company waives any right of subrogation against the United States of America which may arise by reason of any payment under the policy."

(e) When aircraft are used in connection with performing the contract, aircraft public and passenger liability insurance of at least \$200,000 per person and \$500,000 per occurrence for bodily injury, other than passenger liability, and \$200,000 per occurrence for property damage. Coverage for passenger liability bodily injury shall be at least \$200,000 multiplied by the number of seats or passengers, whichever is greater.

**H.16 FINAL SCIENTIFIC AND TECHNICAL REPORTS (NFS 1852.235-73) (FEB 2003)
(ALTERNATE II) (FEB 2003)**

(a) The Contractor shall submit to the Contracting Officer a final report that summarizes the results of the entire contract, including recommendations and conclusions based on the experience and results obtained. The final report should include tables, graphs, diagrams, curves, sketches, photographs, and drawings in sufficient detail to explain comprehensively the results achieved under the contract.

(b) The final report shall be of a quality suitable for publication and shall follow the formatting and stylistic guidelines contained in NPG 2200.2A, Guidelines for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information. Electronic formats for submission of reports should be used to the maximum extent practical. Before electronically submitting reports containing scientific and technical information (STI) that is export-controlled or limited or restricted, contact the Contracting Officer to determine the requirements to electronically transmit these forms of STI. If appropriate electronic safeguards are not available at the time of submission, a paper copy or a CD-ROM of the report shall be required. Information regarding appropriate electronic formats for final reports is available at <http://www.sti.nasa.gov> under "Publish STI - Electronic File Formats."

(c) The last page of the final report shall be a completed Standard Form (SF) 298, Report Documentation Page.

(d) In addition to the final report submitted to the Contracting Officer, the Contractor shall concurrently provide to the Center STI/Publication Manager and the NASA Center for AeroSpace Information (CASI) a copy of the letter transmitting the final report to the Contracting Officer. The copy of the letter shall be submitted to CASI at the following address:

Center for AeroSpace Information (CASI)
Attn: Acquisitions Collections Development Specialist
7121 Standard Drive
Hanover, Maryland 21076-1320

(e) Data resulting from this research activity may be subject to export control, national security restrictions or other restrictions designated by NASA; or, to the extent the Contractor receives or is given access to data necessary for the performance of the contract which contain restrictive markings, may include proprietary information of others. Therefore, the Contractor shall not publish, release, or otherwise disseminate, except to NASA, data produced during the performance of this contract, including data contained in the final report and any additional reports required by 1852.235-74 when included in the contract, without prior review by NASA. Should the Contractor seek to publish, release, or otherwise disseminate data produced during the performance of this contract, the Contractor may do so once NASA has completed its document availability authorization review and the availability of the data has been determined.

H.17 MULTIPLE AWARD CONTRACTS

Orders under this multiple award contract will be placed in accordance with FAR 16.505 and H.8, Task Ordering Procedure. Unless otherwise stated in an individual Task Order Request, the selection criteria to be considered to provide multiple awardees a fair opportunity to be considered for award for each order are: technical approach, cost, and past performance. Unless otherwise stated in an individual Task Order Request, these criteria will be considered of essentially equal importance.

H.18 Reserved**H.19 PROFIT AND FEE ON TASK ORDERS**

Individual cost plus fixed fee Task Orders will be negotiated as a result of proposals submitted for each Task Order. The fixed fee rate accepted or negotiated by the Contracting Officer for the initial requirement under any specific Task Order will be the maximum rate applied to all change or modification actions involving work not previously specified in the Task Order.

H.20 SMALL BUSINESS SUBCONTRACTING PLAN

The Small Business Subcontracting Plan is attached as Exhibit D to this contract. Because of the nature of this contract (i.e., Task Order IDIQ), the Government will annually evaluate the Contractor's performance in meeting the Small Business Subcontracting goals based on the percentages proposed by the contractor in the Small Business Subcontracting Plan.

PART II - CONTRACT CLAUSES

SECTION I - CONTRACT CLAUSES

I.1 LISTING OF CLAUSES INCORPORATED BY REFERENCE

NOTICE: The following contract clauses pertinent to this section are hereby incorporated by reference:

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1)

CLAUSE NUMBER	DATE	TITLE
52.202-1	JUN 2004	DEFINITIONS
52.203-3	APR 1984	GRATUITIES
52.203-5	APR 1984	COVENANT AGAINST CONTINGENT FEES
52.203-6	JUL 1995	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT
52.203-7	JUL 1995	ANTI-KICKBACK PROCEDURES
52.203-8	JAN 1997	CANCELLATION, RESCISSION AND RECOVERY OF FUNDS FOR ILLEGAL OR IMPROPER ACTIVITY
52.203-10	JAN 1997	PRICE OR FEE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY
52.203-12	JUN 2003	LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS
52.204-2	AUG 1996	SECURITY REQUIREMENTS
52.204-4	AUG 2000	PRINTED OR COPIED DOUBLE-SIDED ON RECYCLED PAPER
52.204-7	OCT 2003	CENTRAL CONTRACTOR REGISTRATION
52.209-6	JUL 1995	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT
52.215-2	JUN 1999	AUDIT AND RECORDS--NEGOTIATION
52.215-8	OCT 1997	ORDER OF PRECEDENCE - UNIFORM CONTRACT FORMAT
52.215-11	OCT 1997	PRICE REDUCTION FOR DEFECTIVE COST OR PRICING DATA-- MODIFICATIONS
52.215-13	OCT 1997	SUBCONTRACTOR COST OR PRICING DATA - MODIFICATIONS
52.215-14	OCT 1997	INTEGRITY OF UNIT PRICES
52.215-15	OCT 2004	PENSION ADJUSTMENTS AND ASSET REVERSIONS
52.215-16	JUNE 2003	FACILITIES CAPITAL COST OF MONEY

52.215-21	OCT 1997	REQUIREMENTS FOR COST OR PRICING DATA OR INFORMATION OTHER THAN COST OR PRICING DATA – MODIFICATIONS (ALTERNATE IV) (OCT 1997) Insert (b) Provide information described below: <u>The Contractor shall submit cost or pricing data and supporting attachments in accordance with Table 15-2 of FAR 15.408, unless otherwise stated by the Contracting Officer.</u>
52.216-7	DEC 2002	ALLOWABLE COST AND PAYMENT Insert 30 th in Paragraph (a)(3).
52.216-8	MAR 1997	FIXED FEE
52.217-8	NOV 1999	Option to Extend Services (Nov 99) Insert 30 Days
52.219-8	OCT 2000	UTILIZATION OF SMALL BUSINESS CONCERNS
52.219-9	JAN 2002	SMALL BUSINESS SUBCONTRACTING PLAN (ALTERNATE II) (OCT 2001)
52.219-16	JAN 1999	LIQUIDATED DAMAGES SUBCONTRACTING PLAN
52.222-1	FEB 1997	NOTICE TO THE GOVERNMENT OF LABOR DISPUTES
52.222-2	JUL 1990	PAYMENT FOR OVERTIME PREMIUMS Insert "\$ TBD per task order requiring Contracting Officer's approval" in paragraph (a).
52.222-3	JUN 2003	CONVICT LABOR
52.222-21	FEB 1999	PROHIBITION OF SEGREGATED FACILITIES
52.222-26	APR 2002	EQUAL OPPORTUNITY
52.222-35	DEC 2001	EQUAL OPPORTUNITY FOR SPECIAL DISABLED VETERANS, VETERANS OF THE VIETNAM ERA, AND OTHER ELIGIBLE VETERANS
52.222-36	JUN 1998	AFFIRMATIVE ACTION FOR WORKERS WITH DISABILITIES
52.222-37	DEC 2001	EMPLOYMENT REPORTS ON SPECIAL DISABLED VETERANS, VETERANS OF THE VIETNAM ERA, AND OTHER ELIGIBLE VETERANS
52.223-6	MAY 2001	DRUG-FREE WORKPLACE
52.223-14	AUG 2003	TOXIC CHEMICAL RELEASE REPORTING
52.225-13	DEC 2003	RESTRICTIONS ON CERTAIN FOREIGN PURCHASES
52.225-16	FEB 2000	SANCTIONED EUROPEAN UNION COUNTRY SERVICES
52.227-1	JUL 1995	AUTHORIZATION AND CONSENT (ALTERNATE I) (APR 1984)
52.227-2	AUG 1996	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT
52.227-10	APR 1984	FILING OF PATENT APPLICATIONS-- CLASSIFIED SUBJECT MATTER
52.227-12	JAN 1997	PATENT RIGHTS-RETENTION BY THE CONTRACTOR (LONG FORM)
52.227-14	JUN 1987	RIGHTS IN DATA--GENERAL As modified by 1852.227-14 NASA FAR Supplement (OCT 1995)
52.227-16	JUN 1987	ADDITIONAL DATA REQUIREMENTS
52.228-7	MAR 1996	INSURANCE--LIABILITY TO THIRD PERSONS
52.230-2	APR 1998	COST ACCOUNTING STANDARDS
52.230-3	APR 1998	DISCLOSURE AND CONSISTENCY OF COST ACCOUNTING PRACTICES
52.230-6	NOV 1999	ADMINISTRATION OF COST ACCOUNTING STANDARDS
52.232-9	APR 1984	LIMITATION ON WITHHOLDING OF PAYMENTS

52.232-17	JUN 1996	INTEREST
52.232-22	APR 1984	LIMITATION OF FUNDS
52.232-23	JAN 1986	ASSIGNMENT OF CLAIMS
52.232-25	OCT 2003	PROMPT PAYMENT
52.232-34	MAY 1999	PAYMENT BY ELECTRONIC FUNDS TRANSFER--OTHER THAN CENTRAL CONTRACTOR REGISTRATION
		Insert <u>No later than 15 days prior to the submission of the first request for payment in Paragraph (b)(1).</u>
52.233-1	JUL 2002	DISPUTES (ALTERNATE I) (DEC 1991)
52.233-3	AUG 1996	PROTEST AFTER AWARD (ALTERNATE I) (JUN 1985)
52.233-4	OCT 2004	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM
52.242-1	APR 1984	NOTICE OF INTENT TO DISALLOW COSTS
52.242-3	MAY 2001	PENALTIES FOR UNALLOWABLE COSTS
52.242-4	JAN 1997	CERTIFICATION OF FINAL INDIRECT COSTS
52.242-13	JUL 1995	BANKRUPTCY
52.244-5	DEC 1996	COMPETITION IN SUBCONTRACTING
52.244-6	APR 2003	SUBCONTRACTS FOR COMMERCIAL ITEMS
52.245-5	JUN 2003	GOVERNMENT PROPERTY (COST- REIMBURSEMENT, TIME-AND- MATERIAL, OR LABOR-HOUR CONTRACTS)
52.245-18	FEB 1993	SPECIAL TEST EQUIPMENT
52.245-19	APR 1984	GOVERNMENT PROPERTY FURNISHED "AS IS"
52.246-23	FEB 1997	LIMITATION OF LIABILITY
52.246-25	FEB 1997	LIMITATION OF LIABILITY-SERVICES
52.249-6	MAY 2004	TERMINATION (COST-REIMBURSEMENT)
52.249-14	APR 1984	EXCUSABLE DELAYS
52.253-1	JAN 1991	COMPUTER GENERATED FORMS

II. NASA FAR SUPPLEMENT (48 CFR CHAPTER 18) CLAUSES

CLAUSE NUMBER	DATE	TITLE
1852.203-70	JUN 2001	DISPLAY OF INSPECTOR GENERAL HOTLINE POSTERS
1852.216-89	JUL 1997	ASSIGNMENT AND RELEASE FORMS
1852.219-74	SEP 1990	USE OF RURAL AREA SMALL BUSINESSES
1852.219-76	JUL 1997	NASA 8 PERCENT GOAL
1852.227-70	MAY 2002	NEW TECHNOLOGY
1852.235-70	FEB 2003	CENTER FOR AEROSPACE INFORMATION
1852.243-71	MAR 1997	SHARED SAVINGS

I.2 CLAUSES IN FULL TEXT

The clauses listed below follow in full text:

<u>CLAUSE NUMBER</u>	<u>DATE</u>	<u>TITLE</u>
52.216-18	OCT 1995	ORDERING
52.216-19	OCT 1995	ORDER LIMITATIONS
52.216-22	OCT 1995	INDEFINITE QUANTITY
52.219-4	OCT 2004	NOTICE OF EVALUATION PREFERENCE FOR HUBZONE SMALL BUSINESS CONCERNS

52.219-23	JUN 2003	NOTICE OF PRICE EVALUATION ADJUSTMENT FOR SMALL DISADVANTAGED BUSINESS CONCERNS
52.219-25	OCT 1999	SMALL DISADVANTAGED BUSINESS PARTICIPATION PROGRAM-DISADVANTAGED STATUS AND REPORTING RIGHTS TO PROPOSAL DATA (TECHNICAL)
52.227-23	JUN 1987	SUBCONTRACTS (ALTERNATE I) (AUG 1998)
52.244-2	AUG 1998	CLAUSES INCORPORATED BY REFERENCE
52.252-2	FEB 1998	OMBUDSMAN (ALTERNATE I) (JUN 2000)
1852.215-84	OCT 2003	SMALL BUSINESS SUBCONTRACTING REPORTING
1852.219-75	MAY 1999	

I.3 ORDERING (FAR 52.216-18) (OCT 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from contract award through 60 months from the effective date of the contract.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

I.4 ORDER LIMITATIONS (FAR 52.216-19) (OCT 1995)

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than \$1,000, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) Maximum order. The Contractor is not obligated to honor--

(1) Any order for a single item in excess of \$20,000,000;

(2) Any order for a combination of items in excess of \$20,000,000; or

(3) A series of orders from the same ordering office within 10 days that together call for quantities exceeding the limitation in subparagraph (1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 10 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

I.5 INDEFINITE QUANTITY (FAR 52.216-22) (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after 6 months from the end of the contract period of performance.

I.6 NOTICE OF PRICE EVALUATION PREFERENCE FOR HUBZONE SMALL BUSINESS CONCERNS (FAR 52.219-4) (OCT 2004)

(a) Definition. "HUBZone small business concern," as used in this clause, means a small business concern that appears on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration.

(b) Evaluation preference.

(1) Offers will be evaluated by adding a factor of 10 percent to the price of all offers, except--

(i) Offers from HUBZone small business concerns that have not waived the evaluation preference;

(ii) Otherwise successful offers from small business concerns;

(iii) Otherwise successful offers of eligible products under the Trade Agreements Act when the dollar threshold for application of the Act is exceeded (see 25.402 of the Federal Acquisition Regulation (FAR)); and

(iv) Otherwise successful offers where application of the factor would be inconsistent with a Memorandum of Understanding or other international agreement with a foreign government.

(2) The factor of 10 percent shall be applied on a line item basis or to any group of items on which award may be made. Other evaluation factors described in the solicitation shall be applied before application of the factor.

(3) A concern that is both a HUBZone small business concern and a small disadvantaged business concern will receive the benefit of both the HUBZone small business price evaluation preference and the small disadvantaged business price evaluation adjustment (see FAR clause 52.219-23). Each applicable price evaluation preference or adjustment shall be calculated independently against an offeror's base offer. These individual preference amounts shall be added together to arrive at the total evaluated price for that offer.

(c) Waiver of evaluation preference. A HUBZone small business concern may elect to waive the evaluation preference, in which case the factor will be added to its offer for evaluation purposes. The agreements in paragraph (d) of this clause do not apply if the offeror has waived the evaluation preference.

[] Offeror elects to waive the evaluation preference.

(d) Agreement. A HUBZone small business concern agrees that in the performance of the contract, in the case of a contract for--

(1) Services (except construction), at least 50 percent of the cost of personnel for contract performance will be spent for employees of the concern or employees of other HUBZone small business concerns;

(2) Supplies (other than procurement from a nonmanufacturer of such supplies), at least 50 percent of the cost of manufacturing, excluding the cost of materials, will be performed by the concern or other HUBZone small business concerns;

(3) General construction, at least 15 percent of the cost of the contract performance incurred for personnel will be spent on the concern's employees or the employees of other HUBZone small business concerns; or

(4) Construction by special trade Contractors, at least 25 percent of the cost of the contract performance incurred for personnel will be spent on the concern's employees or the employees of other HUBZone small business concerns.

(e) A HUBZone joint venture agrees that in the performance of the contract, the applicable percentage specified in paragraph (d) of this clause will be performed by the HUBZone small business participant or participants.

(f) A HUBZone small business concern nonmanufacturer agrees to furnish in performing this contract only end items manufactured or produced by HUBZone small business manufacturer concerns. This paragraph does not apply in connection with construction or service contracts.

I.7 NOTICE OF PRICE EVALUATION ADJUSTMENT FOR SMALL DISADVANTAGED BUSINESS CONCERNS (FAR 52.219-23) (JUNE 2003)

(a) Definitions. As used in this clause--

"Small disadvantaged business concern" means an offeror that represents, as part of its offer, that it is a small business under the size standard applicable to this acquisition; and either--

(1) It has received certification by the Small Business Administration as a small disadvantaged business concern consistent with 13 CFR part 124, subpart B; and

- (i) No material change in disadvantaged ownership and control has occurred since its certification;
- (ii) Where the concern is owned by one or more disadvantaged individuals, the net worth of each individual upon whom the certification is based does not exceed \$750,000 after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and
- (iii) It is identified, on the date of its representation, as a certified small disadvantaged business concern in the database maintained by the Small Business Administration (PRO-Net).

(2) It has submitted a completed application to the Small Business Administration or a Private Certifier to be certified as a small disadvantaged business concern in accordance with 13 CFR part 124, subpart B, and a decision on that application is pending, and that no material change in disadvantaged ownership and control has occurred since its application was submitted. In this case, in order to receive the benefit of a price evaluation adjustment, an offeror must receive certification as a small disadvantaged business concern by the Small Business Administration prior to contract award; or

(3) Is a joint venture as defined in 13 CFR 124.1002(f).

"Historically black college or university" means an institution determined by the Secretary of Education to meet the requirements of 34 CFR 608.2. For the Department of Defense (DoD), the National Aeronautics and Space Administration (NASA), and the Coast Guard, the term also includes any nonprofit research institution that was an integral part of such a college or university before November 14, 1986.

"Minority institution" means an institution of higher education meeting the requirements of Section 1046(3) of the Higher Education Act of 1965 (20 U.S.C. 1067k including, a Hispanic-serving institution of higher education, as defined in Section 316(b)(1) of the Act (20 U.S.C. 1101a)).

(b) Evaluation adjustment. (1) The Contracting Officer will evaluate offers by adding a factor of 10 (TEN) percent to the price of all offers, except--

- (i) Offers from small disadvantaged business concerns that have not waived the adjustment;
- (ii) An otherwise successful offer of eligible products under the Trade Agreements Act when the dollar threshold for application of the Act is equaled or exceeded (see section 25.402 of the Federal Acquisition Regulation (FAR));
- (iii) An otherwise successful offer where application of the factor would be inconsistent with a Memorandum of Understanding or other international agreement with a foreign government;
- (iv) For DoD, NASA, and Coast Guard acquisitions, an otherwise successful offer from a historically black college or university or minority institution; and
- (v) For DoD acquisitions, an otherwise successful offer of qualifying country end products (see sections 225.000-70 and 252.225-7001 of the Defense FAR Supplement).

(2) The Contracting Officer will apply the factor to a line item or a group of line items on which award may be made. The Contracting Officer will apply other evaluation factors described in the solicitation before application of the factor. The factor may not be applied if using the adjustment would cause the contract award to be made at a price that exceeds the fair market price by more than the factor in paragraph (b)(1) of this clause.

(c) Waiver of evaluation adjustment. A small disadvantaged business concern may elect to waive the adjustment, in which case the factor will be added to its offer for evaluation purposes. The agreements in paragraph (d) of this clause do not apply to offers that waive the adjustment.

_____ Offeror elects to waive the adjustment.

(d) Agreements. (1) A small disadvantaged business concern, that did not waive the adjustment, agrees that in performance of the contract, in the case of a contract for--

- (i) Services, except construction, at least 50 percent of the cost of personnel for contract performance will be spent for employees of the concern;
- (ii) Supplies (other than procurement from a nonmanufacturer of such supplies), at least 50 percent of the cost of manufacturing, excluding the cost of materials, will be performed by the concern;
- (iii) General construction, at least 15 percent of the cost of the contract, excluding the cost of materials, will be performed by employees of the concern; or
- (iv) Construction by special trade Contractors, at least 25 percent of the cost of the contract, excluding the cost of materials, will be performed by employees of the concern.

(2) A small disadvantaged business concern submitting an offer in its own name shall furnish in performing this contract only end items manufactured or produced by small disadvantaged business concerns in the United States or its outlying areas. This paragraph does not apply to construction or service contracts.

I.8 SMALL DISADVANTAGED BUSINESS PARTICIPATION PROGRAM--DISADVANTAGED STATUS AND REPORTING (FAR 52.219-25) (OCT 1999)

(a) Disadvantaged status for joint venture partners, team members, and Subcontractors. This clause addresses disadvantaged status for joint venture partners, teaming arrangement members, and Subcontractors and is applicable if this contract contains small disadvantaged business (SDB) participation targets. The Contractor shall obtain representations of small disadvantaged status from joint venture partners, teaming arrangement members, and Subcontractors through use of a provision substantially the same as paragraph (b)(1)(i) of the provision at FAR 52.219-22, Small Disadvantaged Business Status. The Contractor shall confirm that a joint venture partner, team member, or Subcontractor representing itself as a small disadvantaged business concern, is identified as a certified small disadvantaged business in the database maintained by the Small Business Administration (PRO-Net) or by contacting the SBA's Office of Small Disadvantaged Business Certification and Eligibility.

(b) Reporting requirement. If this contract contains SDB participation targets, the Contractor shall report on the participation of SDB concerns at contract completion, or as otherwise provided in this contract. Reporting may be on Optional Form 312, Small Disadvantaged Business Participation Report, or in the Contractor's own format providing the same information. This report is required for each contract containing SDB participation targets. If this contract contains an individual Small, Small Disadvantaged and Women-Owned Small Business Subcontracting Plan, reports may be submitted with the final Subcontracting Report for Individual Contracts (Standard Form 294) at the completion of the contract.

I.9 RIGHTS TO PROPOSAL DATA (TECHNICAL) (FAR 52.227-23) (JUN 1987)

Except for data contained on pages 1 through 53, it is agreed that as a condition of award of this contract, and notwithstanding the conditions of any notice appearing thereon, the Government shall have unlimited rights (as defined in the "Rights in Data--General" clause contained in this contract) in and to the data contained in the proposal dated February 7, 2005 upon which this contract is based.

I.10 SUBCONTRACTS (FAR 52.244-2) (AUG 1998) (ALTERNATE I)(AUG 1998)

(a) Definitions. As used in this clause--

"Approved purchasing system" means a Contractor's purchasing system that has been reviewed and approved in accordance with Part 44 of the Federal Acquisition Regulation (FAR).

"Consent to subcontract" means the Contracting Officer's written consent for the Contractor to enter into a particular subcontract.

"Subcontract" means any contract, as defined in FAR Subpart 2.1, entered into by a Subcontractor to furnish supplies or services for performance of the prime contract or a subcontract. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(b) This clause does not apply to subcontracts for special test equipment when the contract contains the clause at FAR 52.245-18, Special Test Equipment.

(c) When this clause is included in a fixed-price type contract, consent to subcontract is required only on unpriced contract actions (including unpriced modifications or unpriced delivery orders), and only if required in accordance with paragraph (d) or (e) of this clause.

(d) If the Contractor does not have an approved purchasing system, consent to subcontract is required for any subcontract that--

(1) Is of the cost-reimbursement, time-and-materials, or labor-hour type; or

(2) Is fixed-price and exceeds--

(i) For a contract awarded by the Department of Defense, the Coast Guard, or the National Aeronautics and Space Administration, the greater of the simplified acquisition threshold or 5 percent of the total estimated cost of the contract; or

(ii) For a contract awarded by a civilian agency other than the Coast Guard and the National Aeronautics and Space Administration, either the simplified acquisition threshold or 5 percent of the total estimated cost of the contract.

(e) If the Contractor has an approved purchasing system, the Contractor nevertheless shall obtain the Contracting Officer's written consent before placing the following subcontracts:

"TBD on a Task Order basis with the exception of those listed in (k) of this clause."

(f) (1) The Contractor shall notify the Contracting Officer reasonably in advance of placing any subcontract or modification thereof for which consent is required under paragraph (c), (d), or (e) of this clause, including the following information:

(i) A description of the supplies or services to be subcontracted.

(ii) Identification of the type of subcontract to be used.

(iii) Identification of the proposed Subcontractor.

(iv) The proposed subcontract price.

(v) The Subcontractor's current, complete, and accurate cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions.

(vi) The Subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract.

(vii) A negotiation memorandum reflecting--

(A) The principal elements of the subcontract price negotiations;

(B) The most significant considerations controlling establishment of initial or revised prices;

(C) The reason cost or pricing data were or were not required;

(D) The extent, if any, to which the Contractor did not rely on the Subcontractor's cost or pricing data in determining the price objective and in negotiating the final price;

(E) The extent to which it was recognized in the negotiation that the Subcontractor's cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the Subcontractor; and the effect of any such defective data on the total price negotiated;

(F) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and

(G) A complete explanation of the incentive fee or profit plan when incentives are used. The explanation shall identify each critical performance element, management decisions used to quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered.

(2) If the Contractor has an approved purchasing system and consent is not required under paragraph (c), (d), or (e) of this clause, the Contractor nevertheless shall notify the Contracting Officer reasonably in advance of entering into any (i) cost-plus-fixed-fee subcontract, or (ii) fixed-price subcontract that exceeds the greater of the simplified acquisition threshold or 5 percent of the total estimated cost of this contract. The notification shall include the information required by paragraphs (f)(1)(i) through (f)(1)(iv) of this clause.

(g) Unless the consent or approval specifically provides otherwise, neither consent by the Contracting Officer to any subcontract nor approval of the Contractor's purchasing system shall constitute a determination--

(1) Of the acceptability of any subcontract terms or conditions;

(2) Of the allowability of any cost under this contract; or

(3) To relieve the Contractor of any responsibility for performing this contract.

(h) No subcontract or modification thereof placed under this contract shall provide for payment on a cost-plus-a-percentage-of-cost basis, and any fee payable under cost-reimbursement type subcontracts shall not exceed the fee limitations in FAR 15.404-4(c)(4)(i).

(i) The Contractor shall give the Contracting Officer immediate written notice of any action or suit filed and prompt notice of any claim made against the Contractor by any Subcontractor or vendor that, in the opinion of the Contractor, may result in litigation related in any way to this contract, with respect to which the Contractor may be entitled to reimbursement from the Government.

(j) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR Subpart 44.3.

(k) Paragraphs (d) and (f) of this clause do not apply to the following subcontracts, which were evaluated during negotiations:

Smart Information Flow Technologies, LLC (SIFT); Scientific Systems Co., Inc. (SSCI); Seagull Technology, Inc.; User Interaction Research and Design, Inc. (UIR&D); Georgia Institute of Technology; Metro Travel.

I.11 CLAUSES INCORPORATED BY REFERENCE (FAR 52.252-2) (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

_____ <http://www.arnet.gov/far/> _____

_____ <http://www.hq.nasa.gov/office/procurement/regs/nfstoc.htm> _____

I.12 OMBUDSMAN (NFS 1852.215-84) (OCT 2003) (ALTERNATE I) (JUN 2000)

(a) An ombudsman has been appointed to hear and facilitate the resolution of concerns from offerors, potential offerors, and Contractors during the preaward and postaward phases of this acquisition. When requested, the ombudsman will maintain strict confidentiality as to the source of the concern. The existence of the ombudsman is not to diminish the authority of the contracting officer, the Source Evaluation Board, or the selection official. Further, the ombudsman does not participate in the evaluation of proposals, the source selection process, or the adjudication of formal contract disputes. Therefore, before consulting with an ombudsman, interested parties must first address their concerns, issues, disagreements, and/or recommendations to the contracting officer for resolution.

(b) If resolution cannot be made by the contracting officer, interested parties may contact the installation ombudsman, Bruce Holmes, direct inquires to Richard Siebels, NASA Langley Research Center (LaRC), Mail Stop 144, Hampton, VA 23681-2199; phone (757) 864-2418; facsimile (757) 864-7709; email Richard.J.Siebels@nasa.gov.

Concerns, issues, disagreements, and recommendations which cannot be resolved at the installation may be referred to the NASA ombudsman, the Director of the Contract Management Division, at 202-358-0445, facsimile 202-358-3083, e-mail james.a.balinskas@nasa.gov. Please do not contact the ombudsman to request copies of the solicitation, verify offer due date, or clarify technical requirements. Such inquiries shall be directed to the contracting officer or as specified elsewhere in this document.

(c) If this is a task or delivery order contract, the ombudsman shall review complaints from Contractors and ensure they are afforded a fair opportunity to be considered, consistent with the procedures of the contract.

I.13 SMALL BUSINESS SUBCONTRACTING REPORTING (NFS 1852.219-75) (MAY 1999)

(a) The Contractor shall submit the Summary Subcontract Report (Standard Form (SF) 295) semiannually for the reporting periods specified in block 4 of the form. All other instructions for SF 295 remain in effect.

(b) The Contractor shall include this clause in all subcontracts that include the clause at FAR 52.219-9.

PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

SECTION J - LIST OF ATTACHMENTS

J.1 CONTRACT DOCUMENTATION REQUIREMENTS

- Exhibit A Contract Documentation Requirements
- Exhibit B Contract Security Classification Specification, DD Form 254
- Exhibit C Safety and Health Plan
- Exhibit D Subcontracting Plan
- Exhibit E IT Security Implementation Plan

EXHIBIT A - CONTRACT DOCUMENTATION REQUIREMENTS

A. Monthly Financial Management Report

1. The Contractor shall submit a monthly financial management report as provided by the Section G clause entitled "NASA Financial Management Reporting." This report shall be submitted utilizing NASA Form 533M, Monthly Contractor Financial Management Report, in accordance with submission instructions contained on the reverse side of the form.
2. For this task order contract, a 533M shall be provided for the levels indicated below:
 - a. Each Authorized Task
 - b. Contract Total. (Column 9b shall reflect total estimated cost of \$# plus fixed fee of \$#.)
 - c. Due not later than the 10th operating day following the close of the Contractor's accounting period being reported.
 - d. Each NF533M shall include a narrative explanation for variances exceeding +-5 percent between estimated dollars shown in the prior month and actual dollars shown in the current month at the total contract level. (For example, the estimated dollars shown for June in column 8a. in the May 533M and the actual June dollars shown in column 7a. in the June 533M.)
3. The minimum reporting categories shall be included in column 6 of this report. Minimum reporting categories shall include:
 - a. Direct Labor Hours
 - b. Direct Labor Dollars
 - c. Overhead(s)
 - d. Subcontract
 - e. Material
 - f. Other Direct Cost
 - g. G&A
 - h. Total Estimated Cost
 - i. Fee
 - j. Total Estimated Cost and Fee

B. Monthly Technical Letter Progress Report -- The Contractor shall submit monthly technical letter reports for each task order describing progress of the task to date, noting all technical areas in which effort is being directed and indicating the status of work within these areas. Tasks may be summarized in one letter report, unless otherwise stipulated in individual task orders. Reports shall be in narrative form, brief and informal in content. These reports shall include:

1. A narrative statement of work accomplished during the report period.

2. A statement of current and potential problem areas and proposed corrective action.
3. A discussion of work to be performed during the next report period.

The monthly progress report shall be submitted within 10 days after the end of each calendar monthly report period. A monthly report shall not be required for the period in which the final report is due.

C. Final Reports -- Each task order may require the Contractor to submit a final report, either formal or informal, which documents and summarizes the results. When a formal final Contractor report is required, it shall be submitted in accordance with the instructions contained in NASA FAR Supplement clause 1852.235-73, Final Scientific and Technical Reports. The specified number of approval copies shall be submitted within the time specified in the task orders.

D. IT Security Implementation Plan. The Contractor shall submit the IT Security Implementation Plan for Contracting Officer and the Langley IT Security Manager approval no later than 30 days after award.

The Contractor shall demonstrate in the IT Security implementation compliance with FISMA, OMB and NIST requirements for IT Security before any remote access is authorized.

The Contractor shall demonstrate in the IT Security implementation plan how computers used to access Langley and other NASA Centers are managed under configuration control using the Center for Internet Security configuration guidelines and how the facility is protected against viruses, worms and other hostile code.

Contractor employees shall obtain Langley RSA tokens for access to the Langley VPN for remote access to Langley NTTS computers. The Contractor shall notify the Langley IT Security Manager immediately upon discovery of a missing RSA token. The Contractor shall notify the Langley IT Security Manager by the close of business of the termination of any employee with a VPN account. (If the employee is to be replaced the RSA token can just be disabled until the new employee is in place, otherwise the RSA token shall be returned to the Langley IT Security Manager within seven days.)

E. Property in the Custody of Contractors (NASA FORM 1018) -- The Contractor shall submit the NASA Form 1018 no later than October 15th of each year in accordance with the Section G clause entitled "Financial Reporting of NASA Property in the Custody of Contractors."

F. Subcontracting Reports

- a. The Contractor shall submit Standard Form 294, Subcontracting Report for Individual Contracts, and Standard Form 295, Summary Subcontractor Report, in accordance with the instructions on the reverse of the forms. In addition to the instructions on the reverse of the SF 295, the Contractor is required to comply with NFS Clause 1852.219-75, Small Business Subcontracting Reporting.
- b. The Contractor shall submit an SDB Participation Report in accordance with the Section I FAR Clause 52.219-25, Small Disadvantaged Business Program -- Disadvantaged Status and Reporting. This report shall be submitted within 30 days after the end of each contract year.

G. Federal Contractor Veterans Employment Report -- In compliance with Clause 52.222-37, Employment Reports on Disabled Veterans and Veterans of the Vietnam Era, the Contractor shall submit the Federal Contractor Veterans Employment Reports (VETS-100) as required by this clause.

H. Evidence of Insurance -- The Contractor shall submit evidence of the insurance coverage, required by the NASA Clause 1852.228- 75 in Section H entitled "Minimum Insurance Coverage" (i.e., a Certificate of Insurance or other confirmation), to the Contracting Officer prior to performing under this contract. The Contractor shall also present such evidence to the Contracting Officer prior to commencement of performance under any options exercised, if applicable.

Sections I-K below pertain to Small Businesses:

I. Interim patent rights report - The Contractor shall submit an annual list of all subject inventions to be disclosed as set forth in FAR 52.227-11 (as modified by 1852.227-11). This report is due every 12 months.

J. Final patent rights report - The Contractor shall submit a listing of all subject inventions or certify that there were none as set forth in FAR 52.227-11 (as modified by 1852.227-11). This report is due prior to contract closeout.

K. Invention disclosure reporting - The Contractor shall disclose each subject invention under the contract as set forth in FAR 52.227-11 (as modified by 1852.227-11). The electronic or paper version of NASA Form 1679, Disclosure of Invention and New Technology (Including Software) may be used for this reporting. Both the electronic and paper versions of this form may be accessed at <http://invention.nasa.gov>. Disclosures are required within two months after the inventor discloses it in writing to Contractor personnel who are responsible for patent matters.

Sections L-N below pertain to Large Businesses:

L. Interim New Technology report - The Contractor shall submit an annual list of subject inventions, certify that all subject inventions have been disclosed (or that there are no such inventions), and certify that the procedures required by NFS clause 1852.227-70 (New Technology) have been followed. This report is due every 12 months.

M. Final New Technology report - The Contractor shall submit a list of subject inventions or certify that there were no such subject inventions, and list all subcontracts at any tier containing a patent rights clause or certify that there were no such subcontracts as set forth in NFS 1852.227-70. This report is due within 3 months after completion of the contracted work.

N. Invention disclosure reporting - The Contractor shall disclose each subject invention under the contract as set forth in NFS 1852.227-70. The electronic or paper version of NASA Form 1679, Disclosure of Invention and New Technology (Including Software) may be used for this reporting. Both the electronic and paper versions of this form may be accessed at <http://invention.nasa.gov>. Disclosures are required within two months after the inventor discloses it in writing to Contractor personnel who are responsible for the administration of the New Technology clause.

II. DOCUMENT DISTRIBUTION REQUIREMENTS

A. Unless otherwise specified elsewhere in this contract, reports and other documentation shall be submitted F.O.B. destination as specified below, addressed as follows:

National Aeronautics and Space Administration
 Langley Research Center
 Attn: _____, Mail Stop _____ [Fill in – See below]
 Contract #: NNL06AA05B
 Hampton, VA 23681-2199

B. The following letter codes designate the recipients of reports and other documentation which are required to be delivered prepaid to Langley Research Center by the Contractor:

1. A--Contract Specialist, Mail Stop 126
2. B--Contracting Officer Technical Representative, Mail Stop 130
3. C--New Technology Representative, Mail Stop 141
4. D--Cost Accounting, NF533@larc.nasa.gov
5. H--Patent Counsel, Mail Stop 141
6. I--Industrial Property Office, Mail Stop 377
7. J--Small Business Specialist, Mail Stop 134
8. K--Center Information Technology Security Manager (CITSM), Mail Stop 124
9. L--According to instructions on form
10. M--As required by Task Order
11. N--Task Monitor
12. P-- Center STI Publication Manager, Mail Stop 196
13. Q-- Industry Assistance Representative, Mail Stop 144

C. The following are the distribution requirements for reports and other documentation required to be delivered f.o.b. destination. The numeral following the letter code specifying the number of copies to be provided:

LETTER CODE AND DOCUMENT: DISTRIBUTION

1. Monthly Financial Management Report (NASA Forms 533M): A-1, B-2, D-2
2. Monthly Technical Letter Progress Report: A-1, B-2, M-1, N-1
3. Informal Final Report: A-1, B-2, C-1, H-1
4. Formal Final Report: As specified by the Contracting Officer
5. Copy of formal final report cover letter: P-1
6. IT Security Implementation Plan: A-1, B-1, K-1
7. Report of Property in the Custody of Contractors (NASA Form 1018): I-1, L

8. Subcontracting Report for Individual Contracts (Standard Form 294) and SDB Participation Report (Optional Form 312): A-1, J-1, Q-1, L
9. Summary Subcontractor Report (Standard Form 295): L
10. Federal Contractor Veterans Employment Report (VETS-100): L
11. Evidence of Insurance Coverage: A-1, B-1
12. New Technology Report/Patent Rights Report: A-1, B-1, C-1, H-1

D. When the Contract Specialist (A) is not designated above to receive a copy of a report or document, the Contractor shall furnish a copy of the report/document transmittal letter to the Contract Specialist. If delegated, the Contractor shall also furnish a copy of the transmittal letter and a copy of each Financial Management Report to the delegated Administrative Contracting Officer of the cognizant DoD (or other agency) contract administrative services component.

EXHIBIT B

Contract Security Classification Specification: DD Form 254

See the next 2 pages.

**DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION**

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

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED

SECRET

b. LEVEL OF SAFEGUARDING REQUIRED

SECRET

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

X	a. PRIME CONTRACT NUMBER NNL06AA05B
	b. SUBCONTRACT NUMBER
	c. SOLICITATION OR OTHER NUMBER
	Due Date (YYMMDD)

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

a. ORIGINAL (Complete date in all cases)	Date (YYMMDD) 060113
b. REVISED (Supersedes all previous specs)	Revision No. Date (YYMMDD)
c. FINAL (Complete Item 5 in all cases)	Date (YYMMDD)

4. IS THIS A FOLLOW-ON CONTRACT? YES NO. If Yes complete the following NAS1-00105, NAS1-00106, NAS1-00107 and NAS1-00108
Classified material received or generated under (see section 13 for Preceding Contract Number) is transferred to this follow-on contract N/A

5. IS THIS A FINAL DD FORM 254? YES NO. If Yes complete the following
In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)		
a. NAME, ADDRESS, AND ZIP CODE Honeywell International Inc. 3660 Technology Drive Minneapolis, MN 55418-1096	b. CAGE CODE 27327	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) Defense Security Services 17177 N. Laurel Park Drive, Suite 417 Livonia, MI 48152-2659

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

8. ACTUAL PERFORMANCE		
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT
FLIGHT CRITICAL SYSTEMS RESEARCH

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		<input checked="" type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		<input checked="" type="checkbox"/>
b. RESTRICTED DATA		<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input checked="" type="checkbox"/>	
d. FORMERLY RESTRICTED DATA:		<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		<input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY		<input checked="" type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)		<input checked="" type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		<input checked="" type="checkbox"/>
(2) Non-SCI		<input checked="" type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		<input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION		<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT		<input checked="" type="checkbox"/>
g. NATO INFORMATION		<input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT		<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION		<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		<input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION		<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		<input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>		l. OTHER (Specify)		<input checked="" type="checkbox"/>
k. OTHER (Specify)					

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public release shall be submitted for approval prior to release

 Direct Through (Specify):

NASA LANGLEY RESEARCH CENTER, M/S 126, HAMPTON, VA 23681-2199
ATTN: C. Lynn Jenkins, (757) 864-3284

To the Office of Public Affairs, National Aeronautics and Space Administration, Washington, DC 20546, for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes: to challenge the guidance or classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any document/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

ALL PERFORMANCE OF WORK FOR THIS PROCUREMENT INVOLVING CLASSIFIED INFORMATION SHALL BE PERFORMED AT GOVERNMENT OR PROPERLY CLEARED CONTRACTOR FACILITIES.

CONTRACTOR SHALL BE PROVIDED CLASSIFICATION GUIDANCE AS NECESSARY TO SUPPORT PERFORMANCE ELEMENTS INVOLVING CLASSIFIED NATIONAL SECURITY INFORMATION.

THE CONTRACTOR FACILITY SECURITY OFFICER (FSO) SHALL CERTIFY THE SECURITY CLEARANCE STATUS OF EMPLOYEES SUPPORTING THIS CONTRACT VIA STANDARD VISIT REQUEST SUBMITTED ANNUALLY OR AS REQUIRED TO THE CERTIFIER IDENTIFIED IN SECTION 16A. THE VISIT REQUEST SHALL INCLUDE THE LEVEL OF CLEARANCE, DATE OF ISSUE, INVESTIGATION TYPE AND DATE COMPLETED.

THE CERTIFIER IN SECTION 16A SHALL BE PROVIDED A COPY OF ANY DD FORMS 254 ISSUED TO SUBCONTRACTORS PERFORMING WORK FOR THIS CONTRACT.

ITEM 10J CONTINUED: INFORMATION EXCLUDED FROM PUBLIC RELEASE UNDER THE FREEDOM OF INFORMATION ACT SHALL BE MARKED "SENSITIVE BUT UNCLASSIFIED".

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

 Yes No

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

 Yes No

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

a. TYPED NAME OF CERTIFYING OFFICIAL

b. TITLE

c. TELEPHONE (Include Area Code)

MICHAEL E. REAGAN

SECURITY SPECIALIST

(757) 864-9470

d. ADDRESS (Include ZIP Code)

NASA LANGLEY RESEARCH CENTER
M/S 301, ATTN: MICHAEL REAGAN
HAMPTON, VA 23681-2199

e. SIGNATURE



17. REQUIRED DISTRIBUTION

- | | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | a. CONTRACTOR |
| <input type="checkbox"/> | b. SUBCONTRACTOR |
| <input checked="" type="checkbox"/> | c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR |
| <input type="checkbox"/> | d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION |
| <input type="checkbox"/> | e. ADMINISTRATIVE CONTRACTING OFFICER |
| <input type="checkbox"/> | f. OTHERS AS NECESSARY |

EXHIBIT C

SAFETY AND HEALTH PLAN

(Revised as of September 30, 2005)

Honeywell's approach to safety and health. Honeywell's Corporate Health, Safety and Environment group provides company-wide safety and health direction. Our commitment to health, safety and the environment is clearly stated by the Corporate Commitment Statement. It opens with this overarching policy: "We are committed to manage health, safety, and environment (HS&E) as a core business value to ensure compliance with all applicable government standards and regulations. We integrate health, safety and environment into all aspects of our businesses as a competitive advantage in achieving profitable growth and accelerated productivity."

One of the goals of the corporate group is to ensure the presence of an HS&E Management System throughout the entire company. The purpose of a formal HS&E Management System is to "institutionalize a company-wide, systematic, well-tested approach to identify and prioritize HS&E risks, identify controls for priority risks, assign responsibility for implementing controls, monitor performance, and continuously improve by learning from ongoing feedback and acting upon it."

The Management System documents explain that Honeywell's approach to safety and health begins with the baseline intention of meeting or exceeding all applicable government, corporate, customer, and site-specific health, safety and environmental expectations. As noted above, we are directed by very specific instructions to conduct and document risk assessments and implement control procedures to maintain a safe situation for our employees, our customers, and our communities. Corporate level policies and procedures describe minimum requirements and may be supplemented by business group safety procedures. Additionally, each facility establishes facility-specific safety procedures whenever the corporate or business group procedures do not fully cover facility procedure needs.

Identifying and mitigating potential safety and health risks. Health, safety and environmental audits are also part of our ongoing management of safety and health. At the facility level, weekly management safety tours are conducted, and resolution of identified issues is tracked. Additional facility-level audits are conducted for specific programs such as energy control, hot work, and line breaking procedures. Formal Honeywell-sponsored annual self-audits of health, safety and environmental programs are conducted by each facility, and the audit reports certified by the highest ranking manager at the facility. A summarized report of self-audit findings is reviewed by the Corporate Audit Committee at the Corporate Board of Director level. Again, issues identified in the self audit are tracked to resolution—both at the site and the corporate level. Every three years, a formal health, safety, and environmental compliance audit is conducted under the auspices of the appropriate Honeywell Business

Group. Finally, yearly fire, boiler, pressure vessel, and business interruption insurance audits are conducted by a consulting arm of our insurance company. Recommendations or non-compliance items from the business group audits and the insurance audits are automatically entered into the corporate HS&E event tracking system and monitored to completion.

The Honeywell Labs facilities have established incident reporting and investigation procedures for all actual or near-miss injuries, illnesses and environmental issues. Participants in incident investigation and remediation include, at a minimum, *affected employees, the occupational health nurse, the facility HSE engineer, and the group supervisor*. Incidents resulting in outcomes that are considered recordable or reportable by government authorities are also entered into the Corporate HS&E event reporting system. To the extent possible, root causes of incidents are identified and site conditions corrected or work procedures revised as appropriate.

Honeywell Labs also has procedures for review of the health, safety and environmental impact of proposed new projects, facility changes and process/procedure changes. Projects new to the facility are reviewed for HS&E concerns and control requirements. Chemicals new to the facility are reviewed for handling precautions, exposure issues, and facility storage and disposal concerns.

The Camden location of Honeywell Labs has an on-site Occupational Health Nurse (OHN) four days per week. The OHN for the facility is a registered nurse. The OHN directs our facility ergonomics program, our first aid team, and manages all medical monitoring programs. The OHN is also the facility contact for workers' compensation management, medical disability, and Family and Medical Leave Act coordination.

The Minneapolis locations of Honeywell Labs are supported by a full-time Health, Safety and Environment Engineer. The HSE engineer is a certified safety professional (CSP) and certified industrial hygienist (CIH). The HSE engineer is the on-site professional most involved in coordinating the HSE Management System activities. The HSE engineer has reviewed NFS 1852.223-70, NFS 1852.223-73, NFS 1852.228-75, NPR 8715.1, NPR 8715.3, and NPR 7100.1. Honeywell's health and safety approach is consistent with these referenced NASA documents. The Honeywell HSE engineer is also available for assistance and consultation on health and safety matters whenever an issue, question, or health and safety need arises.

Honeywell Labs meets the insurance requirements set forth in FAR 52.228-7 clause in regard to "Liability to Third Persons."

For tasks that include experimental flight tests, Honeywell shall perform all analyses and develop all documentation necessary to obtain cognizant safety authority approval as determined by the LaRC Airworthiness and Safety Review Board (ASRB). We will support the Technical Point of contact (POC) and/or COTR in submitting a Flight Test Operations and Test Safety Report (FTOSR) to obtain the appropriate Flight Safety Release letter when work performed under this contract requires experiments to be flown on or involving any aircraft.

Honeywell has prior experience working with the ASRB to obtain approval for experimental flights. We partnered with NASA Langley on the Airborne Information for Lateral Spacing (AILS) / Closely Space Parallel Approaches (CASPER) to develop and test an airborne alerting system. Honeywell supplied NASA with the avionics necessary to flight test the concepts using the NASA 757 aircraft and Honeywell's own Gulfstream-V. The flight tests included Honeywell Gulfstream aircraft flying collision courses with the NASA aircraft and the experimental alerting system detecting the dangerous situation and informing the 757 pilot to perform an emergency escape maneuver. The working system was demonstrated at the Minneapolis/St. Paul International Airport with members of the FAA, industry, and media flying on-board the NASA and Honeywell aircrafts.

On the High Speed Research program, Honeywell supported NASA in obtaining approval for flying the eXternal Vision System (XVS) on the TIFS aircraft, a convair 580 test airplane. This experience plus many years of conducting flight tests on flight control systems for air transport, regional and business jets has prepared Honeywell to effectively prepare analyses and documentation to obtain LaRC ASRB approvals.

IRB for Human Subject Protection. NASA Regulation NPR 7100.1

While performing the proposed work on FCSR for the NASA Flight Critical Systems Research program, the Honeywell team plans to conduct a number of demonstrations and experiments involving human subjects, primarily in evaluating graphical user interfaces and in assessing handling qualities, if needed. The anticipated demonstrations and experiments do not involve invasive procedures, the treatment, cure, or evaluation of any medical conditions, including medical devices or drugs.

Honeywell will retain a registered, qualified IRB for approval and review of the pertinent FCSR experiments and demonstrations to assure that the studies are conducted with the utmost concern for human safety and ethical procedures. Honeywell will provide experimenters with IRB certification training prior to performance of experiments and demonstrations. Honeywell anticipates these experiments and demonstrations to be conducted at Honeywell's laboratory facilities. A letter signed by the Chair of the IRB identifying the proposal submitted to NASA by title and certifying approval of proposed human subjects protocols and procedures will be provided prior to human subject testing.

In summary, we have read and will abide by the requirements laid down in NPR 7100.1 – NASA procedural requirements for the protection of human research subjects.

Summary. Honeywell works actively to identify and mitigate safety and health risks. The well-established processes described above and a team-based approach (that includes the affected employees, the occupational health nurse, the facility HSE engineer, and the group supervisor) along with accountability at the highest level of the company are key to ensuring a safe work environment. Honeywell has experience with utilization of an IRB and the ASRB, and will be proactive in working with NASA to identify and mitigate risks involving human subjects and flight experimentation.

Answers to questions in NPR 8715.3 Appendix H

Honeywell does not expect to occupy facilities on NASA property as part of this project. We acknowledge that NPR 8713.3 applies to Honeywell employees as visitors on NASA property, as noted in section P.2 APPLICABILITY.

Specific answers to the items listed in Appendix H of NPR 8713.3 are detailed below.

- 1.1 Policy. The Honeywell policy statement (see attached) does not vary significantly from NASA and OSHA. NASA's Procedural Requirements are more proscriptive in terms of how the Safety and Health Management System is organized, while Honeywell's policy allows for individual site management structure flexibility. Overarching goals to protect life, health, and property are equivalent.
- 1.2 Goals and Objectives. The specific goals and objectives to be met are no OSHA-recordable injuries and illnesses for any worker involved in the project for the term of the contract. Honeywell project managers have safety and health goals included in their performance evaluation criteria.

- 1.3 Management Leadership. Honeywell is determined to lead the safety program from the top. Each manager is required to have a safety and health goal in his or her performance objectives, and weekly site safety inspections include rotating participation of site managers. Managers also participate in quarterly site safety advisory meetings, safety policy development, and investigation of incidents. The project manager will take personal responsibility for implementation of the project safety requirements.
- 1.4 Employee Involvement. Employees are involved in weekly site safety tours, safety policy development, and first aid response teams for the Honeywell site. Employee involvement for this program will be concentrated on providing appropriate ergonomic design and raising ergonomic and other safety issues for review.
- 1.5 Assignment of Responsibility: Implementation of the safety and health program is the responsibility of the Project Manager. Assistance is provided by the Honeywell Labs Health, Safety, and Environmental (HSE) Engineer, Vicki Chouinard, CIH, CSP.
 - a. The Honeywell Project Manager will be responsible for Honeywell's adherence to Center-wide safety, health, environmental and fire protection concerns and goals. The majority of our work will not be occurring on NASA-controlled sites, so it is not expected that the Honeywell Project Manager will be participating in on-site activities relating to the Center's Safety and Health program. However, the Honeywell Project Manager and Honeywell Labs Health, Safety and Environmental Engineer will be made available for participation as requested.
 - b. The Honeywell physician responsible for this project is
Elizabeth Jennison, M.D.
Associate Director, Medical Services
Honeywell International
101 Columbia Road
Morristown, New Jersey 07962
Telephone: 973-455-3306
 - c. Building Fire Wardens. We do not anticipate occupying a NASA building, and do not anticipate having a Building Fire Warden at the Center. However, if requested, the Honeywell Project Manager will serve to facilitate any appropriate Center's fire safety program responsibilities, including emergency responsibilities.
 - d. The designated safety official is the Honeywell Project Manager. The Honeywell Project Manager will be assisted by the Honeywell Labs Health, Safety, and Environmental Engineer as requested.
- 1.6 Provision of Authority. The Honeywell Project Manager is responsible for maintaining and revising the Safety and Health Plan so that it is consistent with NASA requirements, contractual direction, and Federal, State and local regulations. The Honeywell Labs Health, Safety and Environmental Engineer will be available to provide technical assistance and support as needed.
- 1.7 Accountability. The Honeywell Commitment Statement, the site's Minnesota Employee Right to Know Act procedure, and the site's Cardinal Safety Rules describe how management and employees will be accountable for implementing tasks in a safe and healthful manner. Employees receive training on how to perform jobs safely, they are instructed to discontinue a task if they feel they cannot perform it safely, and safety violations are addressed by the site's overall disciplinary procedures.

- 1.8 Program Evaluation. The Honeywell Project manager will arrange for participation in a PEP survey if requested by the Government. Current ongoing Honeywell program evaluations include completion of a prescribed HSE self assessment tool and annual Assurance letters to the Honeywell Risk Management Committee, regular site visits from Global Risk Services to evaluate facility equipment safety, and a thorough on-site business group HSE audit once every three years. Deficiencies identified in any of these audits are tracked to completion by the Corporate HSE Event Reporting database. Projects that involve new chemicals, new equipment, or changes in equipment, procedures, or chemicals are reviewed by the Facility Manager, who may request formal documentation in a Facility Management Template.
- 1.9 Documentation. Honeywell maintains complete documentation on safety and health policies and procedures. Safety experience metrics, training records, emergency plans, and other documentation are reviewed for completeness and accuracy during the business group audits. These materials will be made available to the government for review and audit when requested.
- a. It is not anticipated that Honeywell activities under this project will be housed on NASA property, nor will Honeywell employees involved in this activity be holders of NASA Center badges. Nonetheless, if information on termination of any employees involved in the project is desired, it will be made available by the Honeywell Project Manager upon request.
 - b. Material Safety Data. It is not anticipated that Honeywell will be supplying any hazardous materials as part of this project. However, if hazardous materials are brought onto Government property as part of this project, MSDSs will be provided as described in Appendix H.
 - c. Hazardous Materials Inventory. It is not anticipated that Honeywell will have any hazardous materials located on Government property as part of this project. However, should the need arise for Honeywell to bring hazardous materials onto Government property as part of the project, a hazardous materials inventory will be maintained by the Honeywell Project Manager. The hazardous materials inventory will include material identity, location and quantity.
- 1.10 Government Access to Safety and Health Program Documentation. All Honeywell safety and health documentation applicable to this project will be made available for inspection or audit at the government's request.
- 1.11 Honeywell will participate, as requested, in review and modification of safety requirements in accordance with established NASA directives and procedures.
- 1.12 Procurement. Materials or services provided by Honeywell contractors are reviewed by the Facility Manager and referred to the Honeywell Labs Health, Safety and Environmental Engineer or the Site Safety Committee as needed. Procurement of services as a part of this project is also covered by standard Honeywell contract safety and health provisions.
- 2.0 Workplace Analysis. As mentioned in the description associated with paragraph 1.3, above, managers participate in weekly site safety tours of Honeywell Labs facilities. Managers also are responsible for participating in supervisor investigations of work-related injuries, illnesses, close calls and incidents. Honeywell Corporate procedures require reporting of injuries, illnesses, adverse environmental events, regulatory actions, audit findings, and citizen concerns. The resolution of these events is tracked to completion. Various hazard identification and ranking procedures are employed including project review by the Facility Manager; personal protective equipment review, chemical hazard control, and energy control review by the health, safety and environmental engineer, and so forth. To the extent the Center's procedures apply, they will be utilized. All hazards associated with this project and identified by Honeywell project participants that are immediately dangerous to life or health will be reported to the NASA safety office immediately.

- 2.1 Hazard Identification. The work Honeywell anticipates providing as part of this contract is expected to be computer design work. Traditional safety hazards to employees working on this project are limited to office hazards and ergonomic hazards. Honeywell will be happy to share information about identified office hazards and employee ergonomic hazards with government representatives upon request.
- a. Honeywell is already completing a wall to wall engineering assessment of the work site as described in the response to paragraph 1.8 above. It is not anticipated that Honeywell will have any facilities, equipment, processes, or materials located on government locations as part of this project.
 - b. Change analysis is a part of our ongoing workplace analysis as described in paragraph 2.0, above. Honeywell Labs HSE Information Update procedure, dated September 3, 2004, requires tracking of regulatory changes so that ongoing regulatory changes can be accommodated. Changes brought about by NASA requirements will be similarly addressed.
 - c. Hazard Analysis. As described in paragraph 2.0, above, hazard analysis is part of our routine safety process. If new facilities, production systems/subsystems, operations, processes, materials, waste, tasks, or jobs are created by Honeywell as part of this project, they too, will be included in our hazard analysis.
- 2.2 Inspections. Honeywell policy calls for a variety of health, safety and environmental inspections. Weekly safety tours are conducted with management and employee representatives. A checklist is used to prompt identification of discrepancies between expected safe conditions and observed unsafe conditions. Weekly inspections of hazardous waste and chemical tank storage areas are conducted and documented. Monthly inspections are conducted for all chemical storage areas and fire extinguishing equipment. Audits of energy control programs, line breaking activities and hot work programs are conducted internally. Internal self-assessments are conducted annually, and business group level health safety and environmental audits are conducted every three years. Employees are encouraged to report hazards informally or formally through near miss forms. All systems have accountability for implementation of corrective measures built into them. Any inspections conducted on NASA property or involving Government furnished property will be similarly documented, and such documentation made available to government representatives as requested.
- 2.3 Employee Reports of Hazards. Employees are encouraged to submit near miss forms as a means of identifying hazardous conditions on the site. Additionally, employees participate in our weekly site safety tours, and are encouraged to bring up safety concerns at that time. All incidents are followed with a supervisor's investigation report, and employees together with supervisors suggest hazard abatement alternatives. Employees may be rewarded for exemplary safety contribution through the Honeywell Bravo award program. Honeywell policy and state OSHA law prohibit employee discipline or discrimination for safety-related activities.
- 3.0 Mishap Investigation and Record Analysis. Mishaps occurring on Honeywell property are investigated through the Supervisor Investigation Report process. Corrective action is tracked through the Honeywell Corporate HSE Event reporting system. It is anticipated that any mishaps involving Honeywell personnel on NASA property or third party property will be treated in a similar manner. As Honeywell will not have dedicated space on NASA property as part of this project, Honeywell staff will be considered to be on travel status when visiting NASA locations. However, Honeywell personnel will be available to participate in NASA investigation, documentation, and corrective action planning following any mishap for which NASA exercises jurisdiction.

- 3.2 Trend Analysis. Trend analysis of data relevant to safety, health, and environmental programs is included when setting managers' goals, specifying safety and environmental training expectations, setting industrial hygiene monitoring schedules, and setting facility action priorities. Incidents are reported to the Honeywell Corporate HSE Event reporting system as they occur, facilitating trend analysis across the corporation. A log of Occupational Injuries and Illnesses is kept at each physical Honeywell location.
- a. If requested to provide an Accident/Incident Summary Report for this project, it will be prepared with the assistance of the Honeywell Labs HSE engineer and delivered by the Honeywell project manager.
 - b. A log of injuries and illnesses for each Honeywell site is maintained as required by Occupational Safety and Health Administration regulations. It is anticipated that Honeywell personnel will not be stationed on government property for more than a year as part of this project, so no separate log of injuries and illnesses will be required. A copy of this location's injury and illness log summary will be provided to the Government upon provision of instructions of where it is to be delivered. Please provide instructions about the injury and illness log delivery to Vicki Chouinard, MN65-1200, Honeywell, 3660 Technology Drive, Minneapolis, MN 55418, 612-951-7168.
- 4.0 Hazard Prevention and Control. Hazards identified, corrective action plans, and completed corrective actions for all Honeywell locations are included in the Honeywell Corporate HSE Event reporting system. We will be happy to provide information needed by the Center's information data system upon request. Please contact the Honeywell project manager or the Honeywell HSE engineer, Vicki Chouinard, with instructions on how/when we should provide information for input into the Center's data system.
- 4.1 Appropriate Controls. Our approach to hazard controls utilizes evaluation of the risk and available control methods. We have a preference for eliminating hazards, designing for minimum hazards, and utilizing engineering controls such as safety and warning devices when they are practicable. In the absence of engineering controls, administrative and procedural controls will be utilized. Some high-hazard procedures such as hot work or live electrical work require documentation on why lower risk activities cannot be substituted for higher risk activities. Control preferences are included in specific Honeywell procedures and in our general management of change process. Coordination with NASA Center facilities and community resources is part of our hazard planning effort. The work Honeywell anticipates providing as part of this project does not use hazardous chemicals or equipment, creates no discharges or waste and generates no hazardous energies.
- 4.1.1 Hazardous Operations. Honeywell does not anticipate performing any hazardous operations as part of this project. Nevertheless, as for all work, the Honeywell Project Manager will be responsible for informing employees, customers, and co-located company representatives of any hazardous operations and the procedures to be implemented to control those hazards. The Honeywell Labs HSE engineer will be available to work with the Honeywell project manager, the government contracting officer, and the NASA Occupational Safety Office to identify hazardous operations and to design appropriate procedures and policies for management and implementation. Information necessary to review adequacy and verify implementation of procedures will be made available to NASA upon request.

- 4.1.2 **Written Procedures.** The Honeywell Corporate procedures cover identification of relevant hazardous situations, proper control methods, inspection, tests and safety documentation. Individual Honeywell Labs procedures provide information necessary to bridge broad Corporate expectations and Site implementation/work assignment needs. The Honeywell Project Manager is responsible for identifying and mitigating hazardous situations. The Project Manager will have the assistance of the Honeywell Labs HSE engineer, and appropriate written procedures will be identified or developed. As mentioned in earlier paragraphs, Honeywell does not anticipate hazardous operations beyond that occurring in an office setting.
- 4.1.3 **Protective equipment.** The Honeywell Labs has a written policy addressing selection, training, inspection and maintenance of protective equipment. This policy will be furnished upon request. However, we do not anticipate that individuals participating in this project will be required to use protective equipment.
- 4.1.4 **Hazardous Operations Permits.** Honeywell acknowledges that it is required to adhere to established NASA Center procedures for hazardous operation permits. At this time we do not anticipate involvement in any hazardous operations. We will not be bringing asbestos to the Center, nor involved in disturbing any existing asbestos the Center might have. We do not intend to undertake operations involving toxic or unhealthful materials. Should we be requested to do so as part of the project we will notify the NASA Occupational Health Office. No hazardous waste generation is anticipated as part of the project. Should project plans change and hazardous waste generation be predicted, the Honeywell Project Manager, the Honeywell Labs HSE engineer, and the Center environmental services office will cooperate to make sure hazardous waste is handled correctly. No new or modified emissions or discharges to the environment are anticipated as a result of Honeywell's work on this project.
- 4.2 **Honeywell does not anticipate occupying facilities at the NASA Center, and does not expect to be performing facilities baseline documentation.** However, if the Center's requirements ask that we complete such tasks, please provide the Honeywell Project Manager with further instruction on requirements.
- 4.3 **Preventive Maintenance.** Honeywell schedules and tracks preventive maintenance for our own facilities and equipment. Safety alerts are circulated within the Honeywell health, safety and environmental engineering community and the facility management community as appropriate. Serious safety alerts or issues often require confirmation of audits or training to the business unit health, safety and environmental manager. Honeywell does not anticipate providing facilities or equipment as part of this project, so does not believe that a description of our preventive maintenance scheduling and tracking process is relevant here. If we do discover design or operational concerns in facilities and equipment related to this project, the Honeywell Project Manager will provide information to the Center's health, safety and environmental departments so that it may be shared appropriately through NASA.
- 4.4 **Medical Program.** Honeywell has a procedure on when medical surveillance programs will be required. We provide medical surveillance when required by Occupational Health regulation (such as for respirator wearers) and when employees are exposed to chemicals for which a medical screening program may be beneficial (such as for those who work with mercury). It is not anticipated that Honeywell personnel involved in this project will be required to participate in any of the existing Honeywell medical surveillance programs. We have an emergency response team trained in CPR, first aid, use of an AED, bloodborne pathogens, and evacuation procedures.

- 5.0 Emergency Response. Honeywell Labs has a written Emergency Action Plan addressing emergency preparedness including fire, explosion, inclement weather, environmental releases and so forth. We regularly remind employees of their responsibilities under the emergency action plan, and conduct storm and evacuation readiness drills yearly. We do not anticipate having any physical presence on NASA center facilities for this project. Any Honeywell employee present at the Center's facilities as part of this project will be covered by the Center's emergency plan as a visitor.
- 6.0 Safety and Health Training. All Honeywell Labs employees receive general information about safety responsibilities and hazard communication. Honeywell Labs has developed a training matrix to identify individuals whose job responsibilities require additional safety or environmental training. Honeywell employees participating in this project will be well served by the general safety training, and no need for specialized safety training is anticipated. At this time, we do not anticipate sending employees through the Center's training resources. The training matrix, training materials, and training documentation is reviewed during Honeywell's business unit HSE audits. These materials will be made available for NASA review on request.
-

Attachments:

- 1) Honeywell corporate commitment statement to Safety and health
- 2) Safety Checklist
- 3) Honeywell Safety Performance Year-to-Date summary
- 4) Health, Safety and Environment bulletin list

Honeywell

Commitment to Health, Safety and the Environment

We are committed to manage health, safety and environment as a core business value to ensure compliance with all applicable government standards and regulations. We integrate health, safety and environment into all aspects of our businesses as a competitive advantage in achieving profitable growth and accelerated productivity.

EMPLOYEES AND OPERATIONS - We seek to protect the safety and health of our employees and minimize our environmental footprint through prevention of illness, injury, and pollution. All employees should be personally involved in furthering this objective.

SOLUTIONS FOR CUSTOMERS AND SUPPLIERS - Health, safety and environment concerns are integral to our processes, services and product designs, including responsible management throughout the product lifecycle. We educate customers, suppliers and the public about the safe use of our products and openly communicate the protective measures we take for employees, our communities, and other key stakeholders.

ACCOUNTABILITY - We utilize management systems to apply global standards, including compliance with applicable laws and regulations. Our executives and managers are measured and held accountable for the safety and environmental performance of their businesses. We hold every employee accountable for his or her role in meeting our commitment.

STAKEHOLDER INVOLVEMENT - We work with stakeholders in the development of laws, regulations and standards that safeguard the community, workplace and environment. As a responsible corporate citizen, we demonstrate this commitment by working within our communities and actively pursuing independent certifications and recognition, as appropriate.

CONTINUOUS IMPROVEMENT - We address occupational injuries and illnesses, emissions, wastes and inefficient use of resources and energy as preventable process defects. We continuously improve our compliance processes and business practices using quantifiable goals to measure and taking actions to drive sustained safety and environmental performance.



Dave Cote
Chairman and CEO
July 2002

Honeywell corporate commitment statement to Safety and health

SBU/Location: _____ Six sigma/Lean Contact: _____
 Project/Activity: _____ Date: _____

This checklist has been designed to help Honeywell employees identify and address health, safety and environmental considerations associated with their projects and activities. The checklist provides a useful framework for building HS&E awareness, anticipating issues and identifying opportunities. You are encouraged to work closely with local HS&E resources starting at the early stages of your project/activity.

Items checked in a shaded area require further investigation or specific actions.

H S&E Considerations				
General	Yes	No	Don't Know	N/A
HS&E resources are consulted up-front in project planning to help identify and resolve potential HS&E concerns and/or identify potential opportunities associated with projects and activities.				
Project members know and understand AlliedSignal's Health, Safety And Environmental Policy.				
Project members are aware that capital appropriation requests MUST include a Health, Safety And Environmental Assessment/Impact Statement				
The HS&E costs associated with the new or modified process(s) have been determined				
Safety				
Written operating and safety procedures have been developed for the new or modified process				
Hazard analysis has been completed for the new or modified processes				
Emergency Response Plan modification required				
Personal Protective Equipment (PPE) requirements have been established (e.g. eye, face, hand, foot, skin, respiratory system protection measures)				
Specific training in safe operation and maintenance procedures are or will be provided and documented				
Guards or other protective devices provided on machinery and equipment				
Work processes have been designed to avoid repetitive lifting, bending, excessive grip strengths and awkward postures				
Safety Declarations And Certificates Of Insurance have been obtained from outside contractors				
Fire extinguishing system additions may be required for flammable or combustible materials control				
Industrial Hygiene				
New or modified processes may increase employee exposure to presently used materials				
New or modified processes may result in exposure to new materials				
New or modified processes and equipment may result in exposure to physical agents (e.g. heat, cold, ionizing and non-ionizing radiation, etc.)				
Noise levels below 85 decibels at operator workstations				
All hazardous materials have been identified and potential routes of exposure assessed and evaluated to ensure they are properly managed				
Hazard Communication training and labeling to inform employees of potential health hazards and precautions have been completed				

Personal Protective Equipment requirements have been specified, communicated and are in place				
Engineering controls (e.g. ventilation systems, process controls) utilized as primary method for minimizing exposures				
Environmental				
New or modified processes may increase or change the characteristics of, existing air emissions, water discharges or wastes generated				
New or modified processes may result in new air emissions, water discharges or wastes generated				
New or modified environmental permits are required				
Additional or new emissions or discharge monitoring is required				
Spill Prevention Plan modification is required				
Local regulatory agency and/or emergency/community response organization notifications are required				
Waste minimization strategies have been identified for each step of new or modified processes				
Opportunities to use less toxic materials and/or prevent waste or emissions generation have been evaluated				
Process recycling and reuse options have been identified				
Toxic Substances Control / Product Safety				
Material Safety Data Sheets and hazard warning labels have been obtained for new chemicals and materials				
Local Chemical Control Committee reviews and approves new process chemicals or other materials prior to use				
New or modified processes may involve import or export of chemicals				
New or modified processes subject to new chemical use notification requirements				
Regulatory product approvals required prior to commercialization of new or modified products (e.g. US EPA, FDA , FAA, DOT; similar international agencies)				
Regulatory requirements exist for product manufacturing, design and performance (e.g. NHTSA, FAA, FDA GMP; similar international requirements)				
Product Stewardship				
New or modified processes/products reviewed to minimize environmental impact and maximize customer value (e.g. Recyclability of products, minimize packaging, use of less toxic materials; "Design For The Environment" & "Design for the Employee" tools used)				
Customer end uses known, reviewed and considered appropriate for use of our products in those applications				
Possible business value from HSE services are evaluated for customers (from value-added services to better support their operations and the use/handling of our products) and for suppliers (from HSE services used to improve supplier productivity and reduce costs).				

Rev. 5 – 7/15/99

Safety Checklist

Honeywell Safety Performance

Jan/2005 through Aug/2005



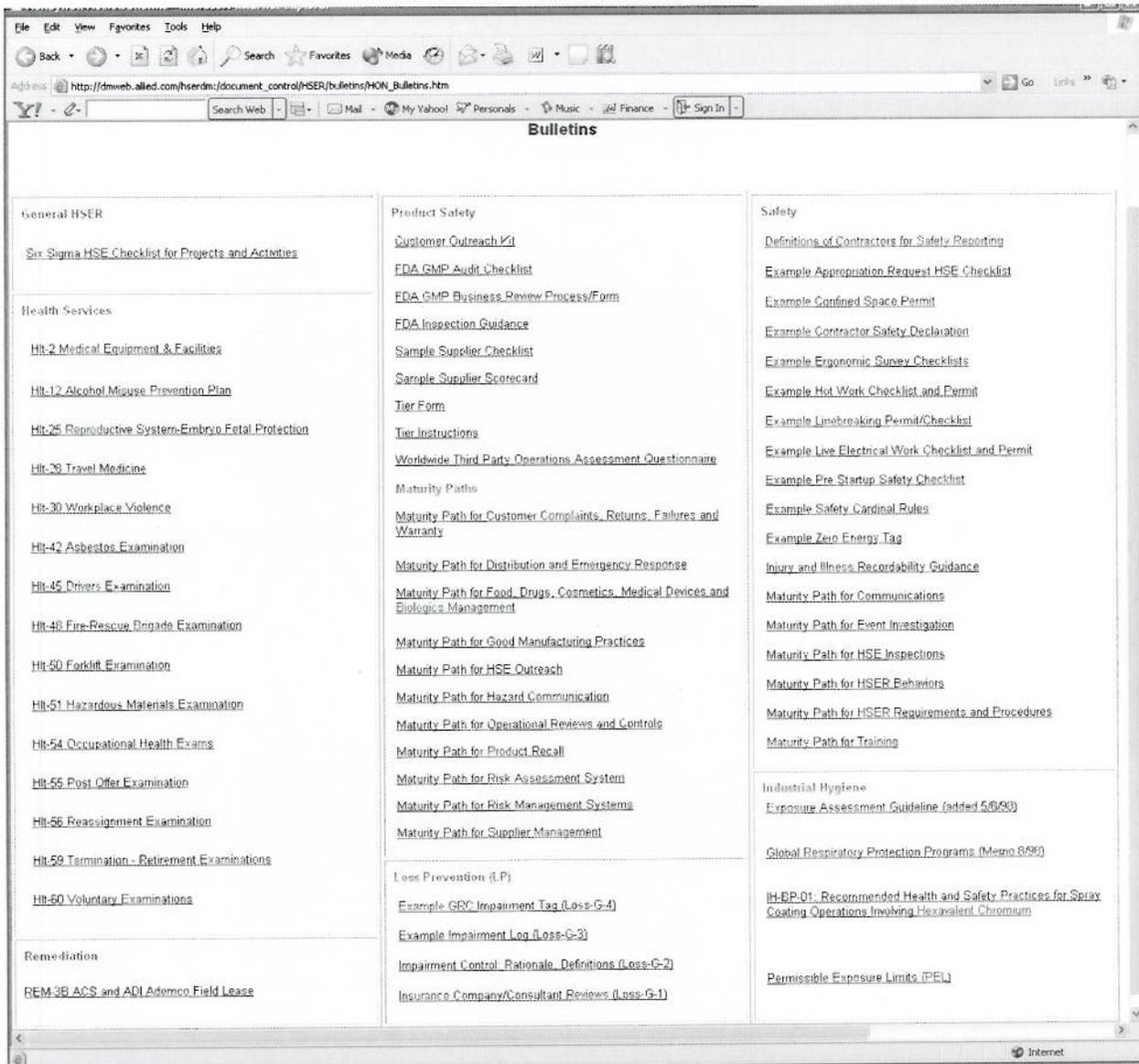
Red = 10% or more than goal
 Yellow = 1 to 9% more than goal
 Green = At or below goal

Sep/27/05

Organization	YTD Exposure Hours	Total Cases	TCIR	Goal	LWCA	LWCAIR	Goal
ECC and S&C [SBU27]	19,406,280	66	0.68	0.79	26	0.28	0.19
HON PROCESS SOLUTIONS [SBU02]	13,466,917	18	0.26	0.18	6	0.08	0.06
HONEYWELL BUILDING SOLUTIONS (HBS) [SBU15]	12,504,182	29	0.46	0.82	9	0.14	0.29
SECURITY & LIFE SAFETY [SBU17]	11,253,963	26	0.49	0.61	3	0.05	0.19
Total for Automation & Control Solutions	56,651,342	141	0.49	0.61	44	0.15	0.18
Total for Honeywell International:	153,717,340	378	0.49	0.60	75	0.09	0.12

TCIR - Total Case Incident Rate
 LWCA - Lost Workday Case(s)
 LWCAIR - Lost Workday Case Incident Rate

Honeywell Safety Performance Year-to-Date summary



Health, Safety and Environment bulletin list

HONEYWELL INTERNATIONAL, INC.
HONEYWELL LABORATORIES

UNDER CONTRACT TO and
IN ACCORDANCE WITH THE REQUIREMENTS OF
NASA
CONTRACT NUMBER NNL06AA64T
EXHIBIT E

IT SECURITY IMPLEMENTATION PLAN

22 MARCH 2006

Contact: Dan Retka, Contracts Manager
Honeywell Laboratories
3660 Technology Drive
Minneapolis, MN 55418
612/951-7854
dan.retka@honeywell.com

Project Support Requirements:

Data exchange between Honeywell and NASA on this project will be limited to e-mail exchange and exchange of files. This purpose of this document is to identify Honeywell's:

1. General security plan and posture
2. Email Messaging Standards
3. Internet Security Protection Plan

General Security Plan and Posture

Honeywell's Information Security Plan is based on a series of individual security policies that are designed to address the ten control areas of the ISO 17799 code of practice for information security management. These policies describe the common protection requirements across Honeywell's business groups including Honeywell Aerospace. The Policies form a baseline for the protection of information resources and a measure from which to gauge each group's effectiveness in implementation. As stated in the Honeywell Corporate Information Security Directive, compliance with the contents is mandatory. Honeywell's computer security policies are compliant with the Computer Security Act of 1987 and have been reviewed against the Federal Information Security Management Act of 2002.

Honeywell Aerospace has a core Information Technology (IT) Security Team Aerospace that partners with the corporate information security team to drive initiatives focusing on awareness, education, compliance assessment, applications security, data security, infrastructure security, and engineering security. Honeywell's Aerospace Information Security Team consists of the following management personnel.

Rich Mason – Director, Aerospace IT Security
James Johnson – Manager, IT Security Audit and Assessments
Jason Lish – Manager, IT Application and Data Security
John Bruggemann – Manager, Engineering IT Security
Tyler Tholen – Manager, IT Security Awareness

E-mail Exchange:

All Honeywell Aerospace e-mail goes through centralized messaging servers supported by Honeywell policy (attached) which addresses server configuration, administration, support, virus protection, and backup/recovery.

Messaging_Servers_
Standard_Rev1_6_30



Exchange of Large Files:

Honeywell Aerospace currently utilizes two main approaches for sharing large files with customers and suppliers. These systems are E-Projects and DEXCenter. Both of these systems are accessible on the Honeywell DMZ and are compliant with Honeywell's International Trade Compliance policies and standards. These servers are supported per Honeywell's Internet Connection Security Standards and Policy (attached) which covers architecture, administration, support, virus protection, incident response, and backup/recovery.

Internet_Connection
_Security_Standards

Internet Connections Security Standards

December, 2002

Global IT Security and Architecture
<http://gsp.honeywell.com/lib/security>

Table of Contents

1	Internet Connections Security Standards	4
1.1	Purpose.....	4
1.2	Scope.....	4
1.3	Compliance.....	4
1.4	Overview – “Zones of Trust”.....	4
2	Architecture for Internet Hosting:	5
2.1	Approved Administration Practices and VLAN.....	6
2.2	Unapproved Infrastructure.....	6
2.3	Standards:.....	7
3	Internet Gateway Standards	7
3.1	Honeywell ITG managed security infrastructure.....	7
3.2	Data must flow through designated access control points.....	7
3.3	Primary Gateway Infrastructure.....	7
3.4	Supplemental Gateways.....	8
3.5	Gateway Management.....	8
3.6	Segregation of Data Flow within a Gateway.....	8
3.7	Internet access configuration requirements.....	9
3.8	Content switches.....	9
3.9	Web caches.....	9
3.10	Screening firewalls.....	9
4	Protected Hosting and Zones of Trust (DMZs)	10
4.1	DMZ Policy and Security Practices.....	11
4.2	No Direct IP Connectivity to the Honeywell Intranet.....	11
4.3	Approved DMZ Systems & Types.....	11
4.4	DMZ Configuration Standards.....	11
4.5	DMZ Configuration Requirements & Types.....	12
4.6	Internet Web Hosting.....	12
4.7	Electronic Mail Messaging.....	12
4.8	Domain Name Service - DNS.....	12
4.9	Extranet.....	12
4.10	Intranet web hosting.....	13
4.11	Services / Protocols.....	13
4.12	Services permitted between Internet and Web Hosting Tier 1 Zone.....	14
4.13	Services permitted between Tier 1, Tier 2, and Tier 3.....	14
4.14	Services that are specifically prohibited between Tier 2 and Honeywell Intranet.....	15
4.15	Modem connections.....	15
4.16	Separation of Development and Production environments.....	15
4.17	Storage of Honeywell Proprietary Information.....	15
4.18	Authorization of customer requests.....	15
4.19	Administrative Access to Web Hosting servers.....	15
5	External Connections – Business Connectivity	17
5.1	Business to Business Connectivity - B2B.....	17
5.2	VPN switches.....	18
5.3	Remote Access Connections.....	18
6	Network Infrastructure Security	20
6.1	Network Configuration and Security Controls.....	20
6.2	VLANs - Virtual Local Area Networks and System Isolation.....	20
6.3	External Firewall, Router and Server Load Balancing (SLB) Switch Configuration.....	20
6.4	Tier 2 Firewall Configuration.....	20
6.5	Firewalls.....	21
6.6	Firewall Rule Management and Default Rules.....	21
6.7	Misuse of Firewall Rules.....	21

7	Systems Configuration Standards and Requirements	22
7.1	Network and Operating System Security	22
7.2	System and Application Administration	22
7.3	System and Application Host Hardening	22
7.4	Virus Controls.....	23
7.5	Patches and/or Upgrades	23
8	Operating System Configuration	23
8.1	General	23
8.2	End-User Authentication	23
8.3	Authentication Access controls	23
8.4	Available Authentication Methods.....	24
8.5	Domain Name Service (DNS) Authentication	24
8.6	Administrator Access	24
8.7	FTP - File Transfer Protocol.....	24
8.8	Time Synchronization	24
8.9	Logs and Auditing	24
9	Process Standards	25
9.1	Change Control.....	25
9.2	DMZ Host Deployment.....	25
9.3	Detective/Preventive Measures	25
9.4	Risk Assessment and Network Vulnerability Scans	25
9.5	Network Intrusion Detection.....	25
9.6	Audit Log Retention and Archiving	25
9.7	Auditing File Access.....	26
9.8	Backup and Recovery	26
9.9	Data Retention	26
9.10	Service Restoration Restriction.....	26
9.11	O/S Restoration from Trusted Sources.....	26
9.12	Security Incident Response Measures	26
Appendix A – Supporting Policy and Standards		27
Appendix B – Definitions		28

Summary of Revisions

Date Approved	Section / Subsection	Overview of Revisions
12/2002		Initial Publication

1 Internet Connections Security Standards

1.1 Purpose

To create and maintain a secure network infrastructure that separates and protects Honeywell's internal network from unauthorized access from the Internet, Extranet and connected 3rd party entities. Use of the specified security practices for establishing gateways, and zones of trust (de-militarized zones - DMZs) to secure the Internet perimeter of Honeywell will be observed.

1.2 Scope

All connections to Honeywell's network perimeter security will follow the approved security standards for the defined connection type when any Honeywell information is transmitted or received within the company or to non-Honeywell business entities. Compliance with Honeywell Information Systems Security Policy and Standards is expected by all Honeywell internal service organizations, and to any contracted service entities that support and/or connect to the Honeywell networking environment.

1.3 Compliance

As stated in policy, all network connections to the Internet are to be authorized and managed by Honeywell. Authorization and Business Unit sponsorship are required as part of a connection request process. Based on the successful passing of a security audit and approval, a subsequent registration of the requested connection will take place. This registration licenses the network connection for continued use and tracks the recorded Business Unit sponsor, purpose, requested life span, approvers, locations, connection type(s), implemented hardware inventory, and associated networked user community. For all network connections requiring a change to the existing infrastructure, an authorized request for connectivity must be completed and change management controls are to be used in the implementation process.

1.4 Overview – “Zones of Trust”

Network security will be established using a “Zones of Trust” method. This model creates secure tiers within the network to stratify and manage the communications traffic. Security controls between the tiers are to contain and direct the flow of data traveling within the network. These restrictions regulate access to only the resources necessary for completion of communications and application transactions. These approved methods of connectivity, products, and security parameters are required for establishing a security compliant implementation in a tiered zone(s) network defense posture.

These security actions include the segmentation of network protocol traffic, hardening of operating systems, applications, databases, and services associated with hosting and supporting business operations for Honeywell. There are specific security requirements for network structures in establishing and maintaining gateways to the Internet. Protected hosting environments will be used to securely position systems and applications within a zone of trust and communicated to an associated network tier. The separation of systems and services by function is how the zones of trusts are securely established. Utilization of network appliances such as switches, routers, firewalls and rules are to be securely configured to support the connectivity standards detailed herein.

2 Architecture for Internet Hosting:

A Zone-of-trust is defined by Honeywell as a set of machines and/or networks that have similar access control requirements based upon users' purposes or data. Default communication links between multiple zones is not allowed. Unless specifically allowed elsewhere, a device must be connected to only one zone. Examples of zones are as follows:

- Internet
- Intranet
- Extranet (3-party connections)
- Application DMZ
- Web Hosting DMZ
- Enterprise Services DMZ (Messaging and DNS)
- Backup Network

A three-tiered architecture will be utilized to deliver distinct security zones of trust within the Honeywell network and establish protected hosting environments. These tiers and corresponding zones of trust, consist of the following segments;

Tier 1 – Web facing layer

Web Servers to be located on the Internet protected by two firewalls configured to allow inbound traffic on ports 80/8080 and 443. FTP services server will also be available at this layer. SMTP servers are allowed for the sole purpose of delivering mail to the approved Honeywell mail systems.

Tier 2 – Application or Business Logic layer

Business logic servers located behind the web servers separated by two firewalls configured to communicate with the web servers on ports needed provide information back to the servers on the Internet tier. The firewall will be configured to block all other requests directly from the Internet and all requests from this layer to the Internet.

Tier 3 – Database layer

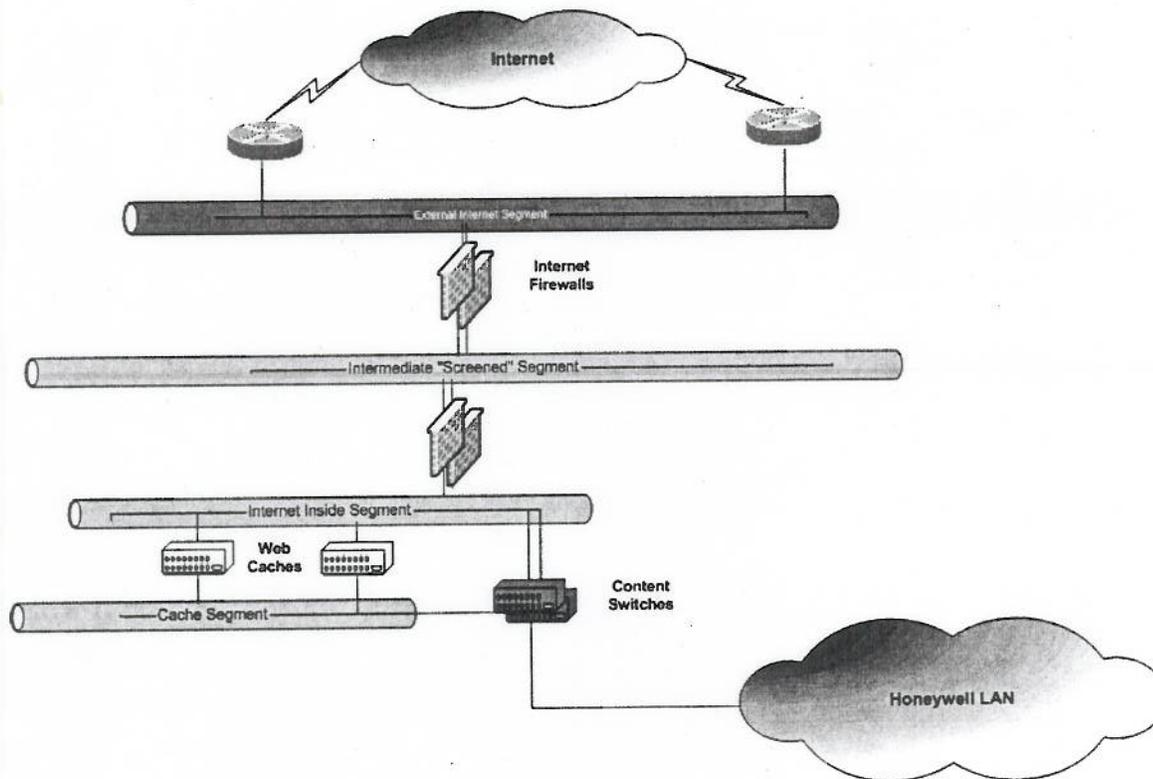
Database servers that provide requested content information back to the web servers based on the information passed to them from the business logic servers. These servers are located behind the business logic servers separated by two firewalls configured to communicate on specific ports and block all unauthorized inbound requests from the Internet.

Dedicated VLANs

Each Tier represented will be isolated to a dedicated VLAN to ensure proper routing and control within the DMZ. The Tier 1 (web facing layer) will be on physically separate switches than the Tier 2 and Tier 3 layers.

Provisions for independent and backup and management VLANs are to be configured to support the secure operating environments detailed herein.

Illustration of Internet Access Architecture



2.1 Approved Administration Practices and VLAN

Administration of the DMZ must be handled by a secure management VLAN segment that is configured to support the following limited functions;

- Server operating systems and security patch updates
- Application management, monitoring and support operations for updates
- Backup and systems management operations

2.2 Unapproved Infrastructure

Tier 1 installations cannot contain any business logic or call databases resident within the same tier. Servers in Tier 1 that include both the business logic and databases on the same server (single platform installations); and servers in any Tier that are dual-homed and therefore bypass the firewalls **are not permitted**.

2.3 Standards:

All new connections of the types previously defined are to include security controls in the forms of firewalls, intrusion detection capability, secure user authentication, and secure data traffic protocols. These security requirements are to utilize the approved architecture, products, and methodologies chosen to meet Honeywell security policy compliance. Additional detail is provided herein. Refer to Appendix A for supporting policy and standards references.

3 Internet Gateway Standards

3.1 Honeywell ITG managed security infrastructure.

Network connectivity gateway standards will address the required technologies to promote a secure computing environment for external commerce and internal services hosting. The utilization of Firewalls (Proxy based and statefull), Gateways, and DMZ network structures will be required. Additionally, Anti-Virus software, security policy management tools and VPN remote access controls augment this infrastructure. Refer to Appendix A for additional supporting policy and standards references.

3.2 Data must flow through designated access control points.

Internet connectivity will route through network and security devices capable of applying and enforcing the traffic controls that are managed by Honeywell. Examples of those capabilities are as follows:

- Identify data stream authentication requirements – Switches, Routers, and Firewalls
- Location specific – Switches, Routers
- User specific – Authentication controls, Network Domain Structures
- Application specific – Proxy Servers, Caching Systems, Content Delivery Networks

3.3 Primary Gateway Infrastructure

Gateway components for Honeywell must be implemented with the following operating characteristics.

- No single point of failure that would not result in the loss of facility
- Backup generator power provisioning for a minimum of 12+ hours
- UPS power, minimum 1+ hours
- No individual components that can have a failure ratio greater of 1%, or maintain 99.9% availability
- Must have maintenance agreements that contain the following requirements:
 - Covers hardware, software and break fix SLAs
 - Minimum 8 x 5 coverage
 - Next business day hardware replacement
 - Must provide primary support in English as well as location local language
- Facility must allow for 7 x 24 hour access availability
 - Facility must have a local shipping and receiving department

- Monitored access control
- Segregated physical access to gateway equipment

3.4 Supplemental Gateways

These gateway installations may be established to support a limited functional list derived from the Primary Gateway characteristics. Implementations of this nature scaled in such manner as to support the limited and identified business requirements.

3.5 Gateway Management

The gateway installation must be able to support a global centralized management model with delineated control standards.

- Rule based access control
- Strong user authentication
- Strong encryption for the management layer
- Centralized logging and local buffering as needed
- Centralized change tracking
- Must be managed from a Honeywell controlled network
- Hierarchical policy management
- Remote console access
 - Fully functional command line abilities

3.6 Segregation of Data Flow within a Gateway

All data flow (inbound & outbound) must traverse a gateway using well defined communication ports and protocols. Refer to document sections 4.11 through 4.14 which cover the specifics for protocols and ports.

Source and destination addresses and ports must be limited to the most restricted access appropriate for a given application. Source and destination addresses and ports used for management processes must be limited to the most restricted access appropriate for a given management solution.

All data flow through a gateway must be IP only.

- All gateway and server management traffic must be encrypted "end-to-end"
- Devices accessed by untrusted devices must be in a DMZ
- Untrusted devices must be in a DMZ
- Data flow must pass through one or more firewalls between a "Zone of trust"

3.7 Internet access configuration requirements

The purpose of this section is to outline special requirements for the components of an Internet access gateway. Provisions are to be made address compliance with the Honeywell security policy for filtering or blocking of non-business related Internet content.

3.8 Content switches

- Redirect web and FTP requests to the web caches for processing.
- Act as non-transparent proxy for web requests to ease migration from existing infrastructure
- Capable of performing transparent load balancing for other services

3.9 Web caches

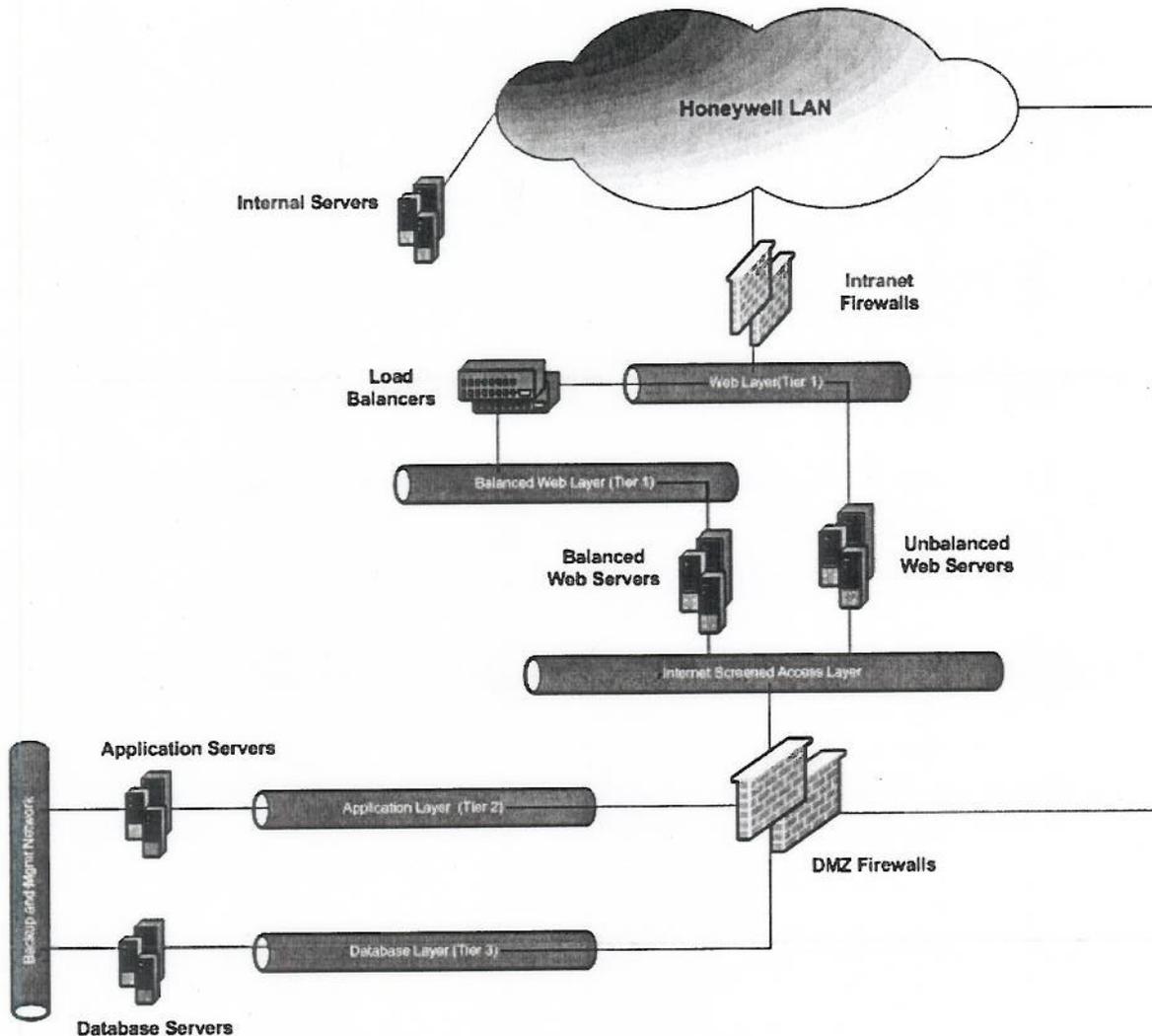
- Perform web caching to increase performance and reduce internet bandwidth utilization
- Capable of performing LDAP based authentication for users requesting content from the Internet
- Capable of providing content screening to prevent inappropriate, potentially offensive or illegal content from being viewed from within the enterprise
- Capable of performing content virus and hostile code scanning on all requested web content

3.10 Screening firewalls

- Control access to the enterprise network by IP addresses and services to strictly control the resources available to the untrusted networks

Control access to the untrusted networks to the greatest extent possible minimizing the enterprises exposure to potentially harmful external locations.

Illustration of Approved Intranet Hosting Architecture



4 Protected Hosting and Zones of Trust (DMZs)

Honeywell interprets the role for a Zone of Trust to be the following:

- A network between its internal network (trusted) and any external network/environment (untrusted)

The role of a secure zone is to separate the internal network from the public (Internet) network. The systems that are placed within the secure zone should not contain confidential or proprietary Honeywell information. This information must remain within an internal network segment whenever possible.

Additionally a DMZ (demilitarized zone) may be deployed to separate certain subnets within the internal network from other portions of the Honeywell enterprise network. Regardless if the DMZ is internal or external configuration requirements outlined within this document are to be followed in order for the DMZ to be approved and deployed.

4.1 DMZ Policy and Security Practices

DMZ policies and standards are the sole responsibility of Honeywell's Global IT Security & Systems Assurance (GSSA). The GSSA are the designated owners of all DMZ policy, configuration and best practices. The following areas will summarize all aspects of Internet Gateway DMZ usage within Honeywell.

4.2 No Direct IP Connectivity to the Honeywell Intranet

Incoming transaction requests must be processed inside the Web facing tier. Connectivity will be accomplished by having all sessions established and controlled by the servers in Tier 1. Data residing on the Honeywell Intranet or the Tier 2, or Tier 3 zone is never directly accessible from the Internet.

4.3 Approved DMZ Systems & Types

Honeywell partitions its DMZ configurations based on identified access requirements. This ensures better protection for the enterprise. Currently there are several approved DMZ types within the enterprise, Internet, Intranet, Messaging, and DNS. The currently approved systems for any DMZ are as follows:

- Internet SMTP servers
- Internet E-Mail Virus scanning servers
- VPN switches
- Internet Web servers
- External DNS servers
- FTP servers
- Intranet Web Servers

Specific descriptions for the DMZ zones characteristics are referenced within this section of the document.

4.4 DMZ Configuration Standards

Regardless of which DMZ type the following system requirements will be implemented:

- Separate network subnets must exist for all DMZ environments
- Hardware based (appliance) firewalls that deploy either fail-over redundancy or high available technology
- Software-based firewall solutions cannot be utilized within any DMZ
- Approved operating systems for DMZ servers are as follows:
 - (Refer to Appendix A for supporting policy and standards references.)
 - Microsoft – NT, Windows2000
 - UNIX - IBM AIX, Sun Solaris
 - Linux – RedHat, SuSe
- Hardening of all operating systems and applications. Refer to a systems hardening section within this document.

- Systems shall not use dual homed network interface cards (NIC) that could bypass any firewall system
- Systems can only be administered via the use of secure authentication on designated VLAN segments within the Honeywell internal network
- Backup of systems can only occur via designated VLAN segments within the Honeywell DMZ network
- Physically separate switching infrastructures must be deployed for internet, intranet, screened access, and DMZ internal networks

4.5 DMZ Configuration Requirements & Types

The purpose of this section to outline special requirements for a particular DMZ type as well as various systems that could be deployed in a given DMZ type.

4.6 Internet Web Hosting

- Three separate tiers: Web, Application and Database
- All web applications must be three tier with separate Web (presentation), Application (business logic), and Database layers. Two tiered applications are permitted, when one or more tiers are absent. Exceptions may be granted for specific types of two tiered implementations such as ASP and are handled on a case by case basis.
- An FTP server is provided in the web for shared use.
- Outbound email must be submitted via the existing Honeywell messaging system using SMTP

4.7 Electronic Mail Messaging

- Relaying must be disabled
- Email must be accepted only for authorized Honeywell DNS domain
- Email must only be sent from an authorized Honeywell DNS domain
- All inbound and outbound must be scanned for virus laden content and hostile code using the ITG approved email scanning solution

4.8 Domain Name Service - DNS

- Split DNS must be used. No internal addresses must be visible to external hosts beyond those authorized to be accessed by those hosts
- Zone transfers must be permitted only with authorized name servers
- No DNS domains must be served externally that are not properly registered and assigned to Honeywell

4.9 Extranet

- Strictly for all contracted 3rd-party vendor/government network communications links
- No other systems can be hosted within this type of DMZ

4.10 Intranet web hosting

- Systems hosted here are restricted to the internal Honeywell network
- No data within these systems can be routed outside the Honeywell network environment with the exception of authorized communications over Extranet and restricted VPN connections

No data from external sources outside the Honeywell environment can be routed to systems residing within this type of DMZ

4.11 Services / Protocols

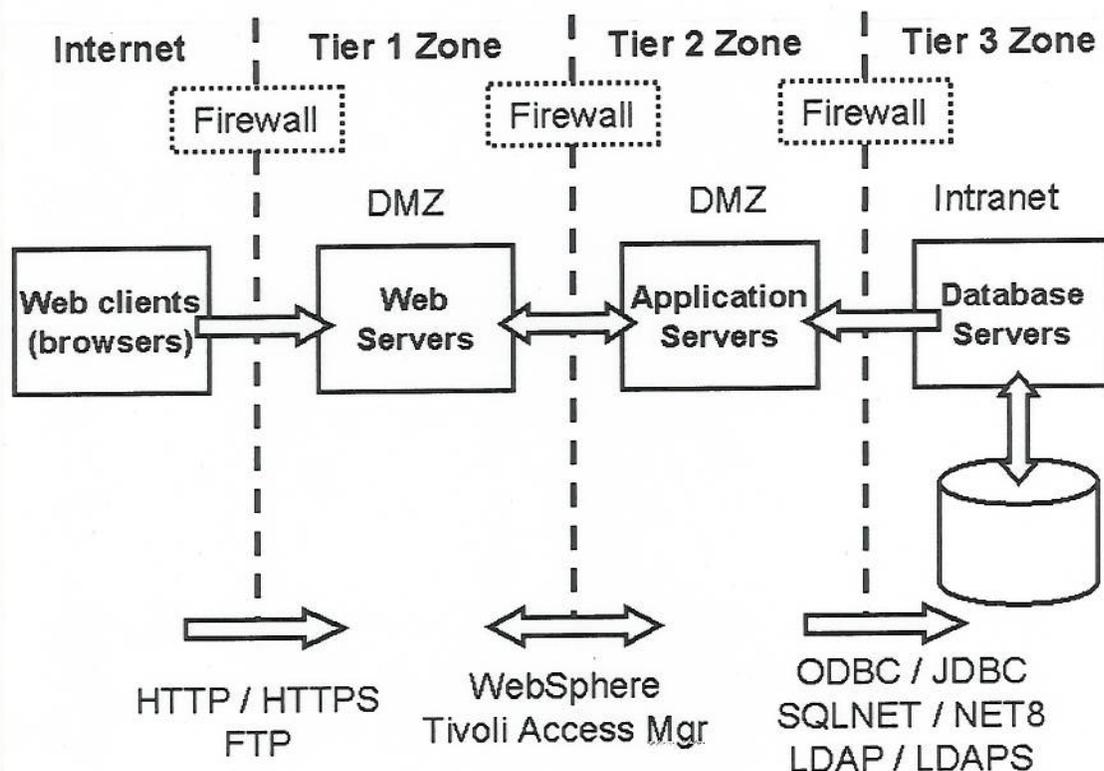
As illustrated in this section, external traffic will not be allowed into the Honeywell Intranet.

Insecure transport services, such as HTTP, should not be allowed through the Tier 1 zone into the Honeywell Intranet. They will not be allowed beyond the Tier 1 zone.

For each application, only one type of service should be allowed through each Zone. The same service should not traverse more than one firewall unless there is extensive filtering/validation of incoming transactions. A list of services, protocols, and ports is provided later within this section.

Therefore, the **basic architectural security model** is to allow HTTPS and HTTP to a server in the Tier 1 zone. The Tier 2 application logic then evaluates the transaction and makes a separate database connection to a database server in the Tier 3 zone. If the database server needs to communicate with the Honeywell Intranet, then the ODBC transaction originates from the Honeywell Intranet. The use of multiple services helps minimize the risk that an attacker can use the same method of compromise across multiple firewalls.

One of the benefits of this model is to reduce the risk of an attack spreading to other systems. If the web server is compromised, the access control between compartments will block all traffic to the database system (except ODBC). As a result, the intruder may be able to attack the database process on the server, but not be able to attack anything else (especially, the Honeywell intranet).



Note: In these diagrams, the arrows show the direction that originates the transaction (data can then flow bi-directionally once the transaction starts). Additionally, the Honeywell web client browser traffic is routed from the Intranet through a separate network connection on the external firewall / router / load balancing switch.

There are several alternatives to this model. In each, the underlying goals are to 1) filter and validate data to remove malicious content, 2) limit the paths of egress into the Honeywell Intranet and 3) use a series of less robust services and application logic that reduce the opportunity for an attacker to penetrate successive zones. In particular, the application's architecture design should not be solely based upon the choice of firewall services, but also include an in-depth analysis of the controls within the application.

Note: XML can be used between the Application server and the Intranet if the Tier1 / Tier 2 servers contain application logic that validates data to remove malicious content and use a series of less robust services.

4.12 Services permitted between Internet and Web Hosting Tier 1 Zone

Only those services required for specific e-Business applications are permitted. "Standard" TCP services currently include:

Service Name	Ports	Protocol Type
HTTP	80/8080	TCP
HTTPS	443	TCP
FTP	20/21	TCP

4.13 Services permitted between Tier 1, Tier 2, and Tier 3

Only those services required for specific e-Business applications are permitted. "Standard" TCP services currently include:

Service Name	Ports	Protocol Type
Oracle SQL*NET or NET8	1521	TCP
MS SQL (ODBC)	1433	TCP
LDAP / LDAPS	389	TCP
RMI over IIOP		TCP
SCP (as replacement for FTP)	22	TCP
Tivoli Access Manager	4441/4442/4443	TCP

At the discretion of GSSA other application services may be permitted.

4.14 Services that are specifically prohibited between Tier 2 and Honeywell Intranet

Services that are not permitted include, but are not limited to the following:

Prohibited Services	Prohibited Services	Prohibited Services	Prohibited Services
NIS	TFTP	BGP	Ntalk
Echo	Finger	exec	Uucp
Qotd	rlogin	login	Listener
lockd	RPC	shell	Active Directory
Teinet	netbios	Talk	NFS
DNS	NNTP	Portmapper	Xwindows
DCOM			

4.15 Modem connections

No modem connections are allowed to servers within the Tiers 1, 2, and 3 environments.

4.16 Separation of Development and Production environments

Systems development activity must be separate from the live operational environment, ideally using separate computing system platforms. There are to be controls to prevent and detect the introduction of unauthorized 'executables' (i.e., computer viruses, Trojans, or other unauthorized code). Additional restrictions for access to source code software and documentation are to be addressed.

4.17 Storage of Honeywell Proprietary Information

Honeywell Proprietary information must be stored in the Tier 3 zone or the Honeywell Intranet. Similarly, application software, and business logic, other than administrative software and CGI scripts, must be stored in the Tier 2 zone.

4.18 Authorization of customer requests

Transactions that originate from the Internet are inherently dangerous. More stringent security is placed on services required between Tier 1 and Tier 2 zones. If the customer request is not standard, i.e., not covered in this document, then the criteria for evaluating this request follows.

- The application should use a single (or small range of) "registered" TCP ports.
- The application should communicate with a single (or small number range of) Honeywell IP address(es).
- Unfiltered transactions **are not allowed** into the Tier 3 zone or the Honeywell Intranet.

4.19 Administrative Access to Web Hosting servers

Configuration and administration of the Web Hosting servers is only allowed from the console or specific IP addresses on the Honeywell Intranet using Radmin, or Secure Shell (SSH) and must be used to provide an encrypted and authenticated transmission channel.

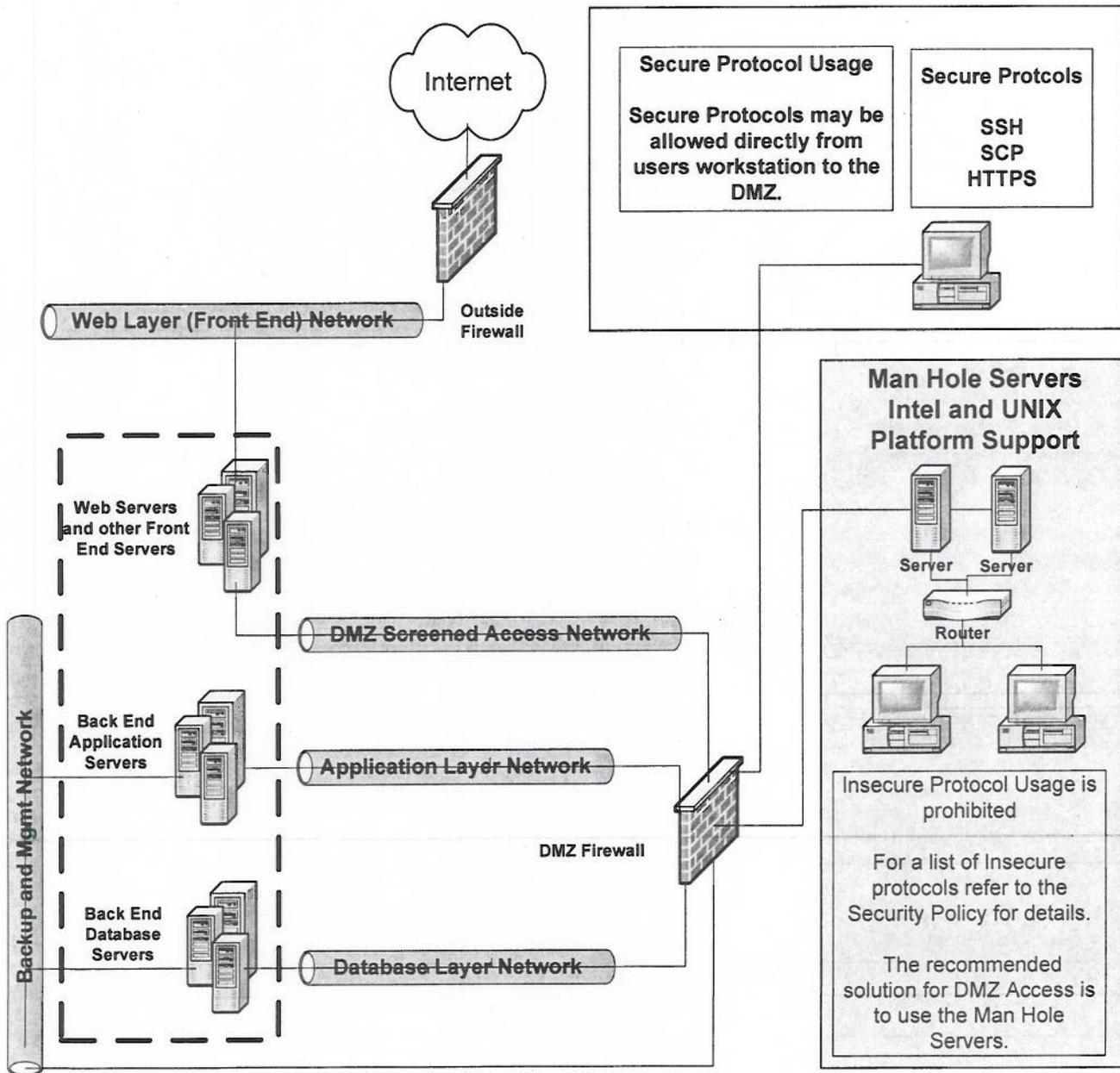
Administrative access for application software that cannot run remotely under Radmin, or SSH, must have the same security equivalency and be supportable by GSSA. The utilization of PCAnywhere is only permitted by approved policy exceptions.

Remote access to the Honeywell network must utilize the established VPN connectivity solution. Remote configuration or administration from the Internet is not permitted.

The preferred method for administration of system within the secured zones or DMZs is to utilize the Man Hole servers that support those services for the Intel and Unix platforms and operating systems. Refer to the illustration for the established access architecture for administration of systems located within the secure zones, DMZs.

Refer to illustration on access architecture for system administration within the DMZs.

Illustration of access architecture for system administration within the DMZ.



5 External Connections – Business Connectivity

5.1 Business to Business Connectivity - B2B

In addressing the multiple connection requirements for Internet, Intranet, and Extranet services to 3rd party connectivity, the secure defensive layering topology is to be implemented as specified. This documentation is referenced for the approved methods of connectivity, products, security parameters required for a security

compliant implementation in a tiered zone(s) perimeter defense posture. See Appendix A for associated policy and standards references.

5.2 VPN switches

- Provide secure remote access to Honeywell networks for authorized personnel using IPSec, PKI, and strong encryption
- Provide secure enterprise network extensions to remote Honeywell offices using IPSec, and strong encryption
- Provide restricted access to authorized third-party locations using IPSec, and strong encryption limiting access to only the approved devices and services

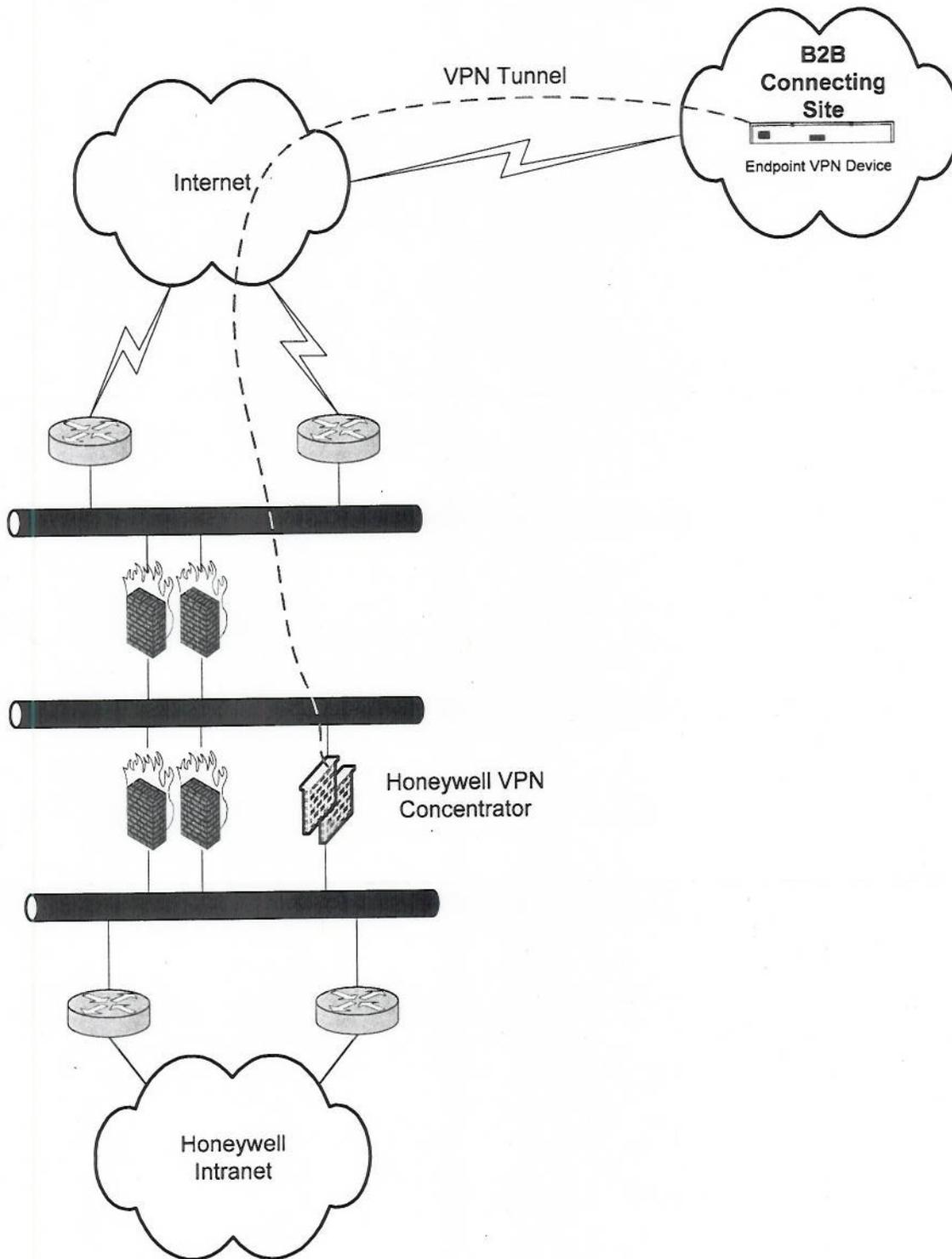
5.3 Remote Access Connections

The established secure VPN connectivity methods are to be employed for remote access. Individual users are to have a specific VPN account established by their individual identity and be issued a specific certificate associated with the installed VPN client to access Honeywell networks and systems.

- **Business to Business (B2B) connections**

The connection solutions for B2B VPN connectivity will be based on the Honeywell ITG GSSA vendors for VPN switches. We have established support agreements with VPN product vendors that meet our security standards. Use of different products could potentially limit the ability of ITG GSSA to support and troubleshoot B2B connections. It should be mentioned that we have established other B2B connections with various VPN-capable devices. The specifications are part of the technical standards required by Honeywell to negotiate working VPN connectivity in a B2B setting.

Illustration of VPN connection architectures



6 Network Infrastructure Security

The network security controls for the infrastructure delineate the permissible architecture and configurations to support the Internet and Intranet connectivity in a manner that is in compliance with the security policy. Refer to Appendix A for supporting policy and standards references.

6.1 Network Configuration and Security Controls

Firewalls and filtering routers are positioned to control information flows between the Internet, the Web Hosting, and the Honeywell Intranet. Access Control Lists - ACLs will be configured to filter traffic and block unauthorized access. Only those services required for specific Web applications are permitted. The Web Hosting provides multiple levels of security for different tiers of applications (front end web servers, application servers, database servers, back end systems on the Honeywell Intranet). Therefore, there are different zones that contain servers of similar security requirements and functionality. Servers shall be connected across only the designated VLANs. Servers within the hosting environment shall never be connected either to unprotected network segments or to the intranet itself.

6.2 VLANs - Virtual Local Area Networks and System Isolation

Within the Web Hosting, all systems must be isolated from each other so that the risk of a wide spread security breach is minimized. For example,

- Virtual Local Area Networks (VLAN) and firewalls are used to isolate each application server or logical group of application servers.
- Routing and switching are not permitted between VLANs within the hosting environment – all traffic traversing VLANs must pass through one or more firewalls.
- Firewall rules and Access Control Lists (ACLs) on network equipment are used to limit those IP Addresses that are allowed to perform remote administration and monitoring.

6.3 External Firewall, Router and Server Load Balancing (SLB) Switch Configuration

The external facing router/firewall/switch is configured to:

- Allow inbound connections from the Internet to specific IP addresses in Tier 1 only.
- Identify, log, and drop any unauthorized connection originating from a Tier 1 server.
- Log all unauthorized HTTP and FTP access attempts. (Keep a minimum log of one week on-line and six month's off-line).
- Generate an alert for all unauthorized access attempts from Tier 1 to the Internet.

6.4 Tier 2 Firewall Configuration

The Internal Tier 2 firewall is configured to:

- Allow inbound and outbound connections to specific IP addresses only. Only allow cross zone traffic (from and to Tier 1 and Honeywell Intranet).
- Internal firewalls are to use a firewall product technology that is different from the Internet facing firewall.
- Generate an alert for all unauthorized access attempts from/to Tier 1 or to the Honeywell Intranet. (Keep a minimum log of one week on-line and six month's off-line).

6.5 Firewalls

All Internet and internal DMZ firewalls shall be redundantly deployed to ensure availability and provide resistance to single points of failure. The gateway firewalls shall be a network appliance (hardware), instead of a UNIX or NT server running firewall software. GSSA is responsible for all maintenance and configuration of all gateway firewalls. Internal network firewall responsibility may be handled by departments other than GSSA based on need. The Honeywell Intranet Firewall is configured to:

- Only allow inbound connections from Tier 1 and Tier 2 servers to specific IP addresses in the Honeywell Intranet.
- Allow any address in the Honeywell Intranet to connect to a Tier 1 server.
- Generate an alert for all unauthorized access attempts from Tier1 or Tier 2 to the Honeywell Intranet.
- Log all attempted accesses to other than authorized e-Business applications. (Keep a minimum log of one week on-line and six month's off-line).

6.6 Firewall Rule Management and Default Rules

Honeywell corporate firewall settings are presently controlled by the Global IT Security Firewall Management team. The requesting of new or changes to the present FW rules is facilitated by an established process. The Firewall Rule Request (FWRR) process is available on the Honeywell Intranet at the following location:
<https://security.honeywell.com/firewall.htm>

Firewall requests will be individually reviewed and approved or rejected based upon need and security concerns. Requests which are required for application operation and do not pose undue risk to the enterprise or the enterprise's intellectual property, and do not violate policy will be approved and implemented.

Access control changes must be submitted via the ITG Firewall Rule Request ([FWRR](#)) web site only.

6.7 Misuse of Firewall Rules

No "port forwarding" or "tunneling" is allowed between the Web Hosting and the Honeywell Intranet. Application Developers must never subvert firewall controls by using a service over a non-standard TCP or UDP port. Honeywell Global IT Security must approve all requests for applications to use non-standard port numbers. Requests for utilization of non-standard services and ports must be submitted using the Firewall Rule Request process.

7 Systems Configuration Standards and Requirements

7.1 Network and Operating System Security

All operating systems, databases, and other software associated with web hosted applications must be secured to reduce the threat of an attack. Industry "best practices" will be used to acquire configuration settings that are not identified in the Honeywell Information Systems Security Policy and Standards.

7.2 System and Application Administration

All servers placed within an Internet DMZ are required to deploy a secure authentication methodology and operate within the existing security policy for Administration policy and standards. The administrators can only perform their support via the internal network.

- No remote administration can occur via the Internet unless a connection is established via the Honeywell supported VPN services.
- Only the Honeywell approved remote administration tools may be used
- Direct root or administrator access shall not be performed – any functions requiring superuser access shall be performed using sudo or similar tool where possible. If not possible, the administrative user shall first authenticate as a named user and then become the superuser to maintain proper audit trail.

The approved access method for systems administration will be followed. Utilization of the "man-hole" access servers to facilitate this access is required.

7.3 System and Application Host Hardening

All hosts to be deployed or within the hosting environment shall be hardened against malicious attack. Hardening is done at two different levels: application and operating system. Below are references to documents that detail the hardening requirements. Before a host can be deployed on a DMZ, it shall meet the requirements set within its corresponding security hardening documents.

- [Security Hardening for Windows NT Servers](#) - Available now
- [Windows 2000](#) -Available now
- [Security Hardening for IBM AIX](#) – Available now
- [Security Hardening for Sun Solaris](#) – Available now

In general, the hardening process includes controlled installation, removal of unnecessary software, and disabling the applications, services, and daemons which increase risk of compromise. Examples include disabling windows file sharing, turning off small TCP services, not running SMTP servers that accept mail from remote hosts, and removing X11 windows system packages since there is no graphics display installed.

Hosts that are deployed on a DMZ must be verified by Global IT Security Risk Assessment prior to production use. A process to securely promote systems into the secure network zones has been developed and is referenced in the Processes section of this document. Systems hardening documents can be referenced at the Global IT Security site:<http://qsp.honeywell.com/sc>

7.4 Virus Controls

Controls to prevent the transmission of malicious code to customers and Honeywell personnel must be implemented. Virus scanning software will be installed and used on every server. The specifics for the virus scanning tools for each operating system and platform can be found at <http://gsp.honeywell.com/lib/infrastructure>. See platform specific standards for associated product offerings. This is a requirement for every server within the Honeywell network.

7.5 Patches and/or Upgrades

Industry vulnerability warnings **will be** monitored by GSSA, E-Business and application owners. The latest security patches **will be** installed as soon as possible. If software must be upgraded to address security vulnerabilities, the upgrade must be done in a time frame that is reasonable and mitigates risk.

8 Operating System Configuration

8.1 General

- File permissions across the server shall be carefully controlled to minimize exposure of the operating system.
- Anti-virus software shall be installed, maintained, and properly configured.
- Web servers and other application based functions shall run as non-privileged users.
- Only web content shall be present in directories accessed by the web server for content.
- Web server executables – i.e., CGI scripts – shall be contained within subdirectories specifically designated to hold scripts. They shall never be installed in any directory holding static content and shall not be retrievable using user-facing applications.
- World writeable directories or Everyone (Windows NT) permissions shall not be used.
- Network shares or file sharing in general using NFSv2, Novell, or NT are not allowed.
- Security settings for all Web directories should be reviewed and adjusted appropriately. The web server user shall not be permitted to write files to the web content directories – only to the log files.
- There must not be a trust relationship with any other machine. If a web hosting server is compromised, it must be unable to be used to obtain access to other machines.

8.2 End-User Authentication

All users must be securely authenticated before allowing access to Honeywell Proprietary or other restricted access information. Resource owners must classify and label confidential and/or proprietary Information as identified by Honeywell Information Systems Security Policy and Standards.

8.3 Authentication Access controls

User authentication information shall be protected when transiting networks using appropriate 128bit encryption such as SSL. NT credentials shall not be passed over untrusted networks – although it is permissible to pass NT authentication information within SSL.

Passwords must be stored in an encrypted form in the Tier 2 or Tier 3 zones of the Web Hosting or the Honeywell Intranet. Refer to, "Administration - General" in Honeywell Information Systems Security Policy and Standards documentation.

End-user authentication information may be stored on a Tier 1 server only if the application being requested is located solely within the Tier 1 zone.

8.4 Available Authentication Methods

The use of centralized web authentication methods is preferred. The following are examples of user authentication methods to control access to various levels of Honeywell confidential and/or proprietary information:

- Hardware token-based authentication (i.e., SecurID passcode generators, smart cards)
- Personal digital certificate authentication using Public Key Infrastructure (PKI)
- Static user IDs and passwords
- Session tracking using session cookies following successful authentication using one or more of the above methods.
- Below are examples of technologies that shall not be used:
- Encrypted or non-encrypted persistent cookies
- Hidden fields in HTML POST methods
- URL tracking
- Windows domain or other trust relationships.

8.5 Domain Name Service (DNS) Authentication

DNS must not be used for authentication purposes.

8.6 Administrator Access

On UNIX systems, administrators should login with their regular accounts and then use the "su" command if they need root access. This way each time someone executes "su", a log entry is generated providing a security audit trail. Direct root logins shall not be permitted. Use of "sudo" is encouraged when feasible.

8.7 FTP - File Transfer Protocol

From the Internet, the FTP service is only permitted on Tier 1 servers. If an FTP service is necessary, then consider the following approaches to protecting the integrity of the server:

- No FTP service to a Tier 2 or Tier 3 server is allowed.

8.8 Time Synchronization

Time synchronization is extremely important when attempting to recreate composite events following suspicious activity and for root cause analysis following problems. To aid in this, all devices deployed within the hosting environment shall be synchronized to a centrally managed time distribution service. This should generally be the Network Time Protocol (NTP) from the designated time servers. If precision time synchronization is required, it is permissible to use a GPS-based time source either locally or within the hosting facility.

8.9 Logs and Auditing

All systems deployed within the hosting environment shall have appropriately configured logging and auditing to permit the subsequent analysis by GSSA or other authorized locations. Logs shall be maintained by the operating system and may be retained off platform as well. Logs shall be protected to aid in integrity validation.

9 Process Standards

9.1 Change Control

To ensure that all application elements are version controlled and that changes can be attributed to identifiable individuals, Honeywell change control process will be used to control, review, approve and log all changes to an Web Hosting server and/or application.

- All changes to the firewalls and e-Business Hosting servers **will be** strictly controlled and approved by all involved parties (GSSA, Application Team, IBM). Service Center will be the tool used to track changes.
- Financial "quiet times" will be observed.

9.2 DMZ Host Deployment

The deployment of systems into established internet/intranet secure hosting zones will follow an established procedure to address appropriate operating systems and applications security. This process is inclusive of phases that identify the process of building, testing, security scanning, review of vulnerabilities and aberrant security settings, corrections, and the subsequent promotion of those systems into the designated network area.

The Systems Security Promotion Process details are available on the Honeywell Intranet at the following location: <http://gsp.honeywell.com/sc>

9.3 Detective/Preventive Measures

A process of post-deployment systems monitoring for security is established to police internet/intranet applications and services for the appropriate security controls. GSSA will follow an established procedure to address appropriate operating systems and applications security using intrusion detection systems, security policy monitoring and vulnerability scanning services.

9.4 Risk Assessment and Network Vulnerability Scans

GSSA has responsibility for scanning networks, machines and applications in the Internet and Intranet networking infrastructure and associated subnets on the Honeywell Intranet. During the deployment process and on an ongoing basis, security scans will be performed on the machines that support the application and vulnerabilities that are found, are to be mitigated and resolved. This activity will identify systems with: aberrant security settings, hosts that either fell out of compliance or were deployed without proper procedure and are now in a non-compliant security state.

9.5 Network Intrusion Detection

GSSA will install network intrusion devices and applications to aid in monitoring potential security breaches and emergency response. These actions will occur as the security for the network zones continue to develop.

9.6 Audit Log Retention and Archiving

Audit/event logging procedures that preserve the integrity of logs should be used such that there are routinely backed-up copies of all logs available and stored off the system.

- Logs (and spool directories) are kept on dedicated disk partitions to reduce the effect of them filling up the rest of the system.
- Transmit the archived audit logs from the host to backup media or to another machine on the Honeywell Intranet.
- Capacity management for disk utilization is to be observed. When usage reaches approximately 90% capacity, evaluate the situation and take appropriate action so that new auditing and security logs are not lost or overwritten.
- Retention requirements for security logs are one year (if possible). Otherwise, keep a minimum log of one week on-line and six month's off-line.

9.7 Auditing File Access

Audit the access of selected files and directories to determine whether anyone has gained unauthorized access to sensitive files. Periodically, review the audit records to check for unauthorized access.

9.8 Backup and Recovery

Disaster recovery plan needs to be defined by the Application owner. Back-up versions of essential information and software should be maintained for the designated retention periods, preferably using an automated process. If the application does not require backup, then backups are not required solely for Audit log purposes.

9.9 Data Retention

Data retention requirements for application data, transaction records, and business continuity backups are regulated by the Honeywell Retention Policy and standards for platform integrity controls. These are documented and available for review. Refer to Appendix A for the supporting policy and standards.

9.10 Service Restoration Restriction

Application owners are responsible for identifying data backup and disaster recovery requirements. They are also responsible for developing Business Contingency plans supporting the applications deployed in the secure Internet zones.

9.11 O/S Restoration from Trusted Sources

Operating system restores must only be performed from original vendor media or archived backups that were created after the original installation, and before any system compromise condition was detected. This will enable the machine to be recovered if a system is detected of being compromised.

9.12 Security Incident Response Measures

In the event of a security related incident, or you suspect a compromise has taken place on the system or to the resident application, contact Global IT Security & Risk Assessment to conduct a system review. The Incident Reporting process is hosted in the Honeywell Intranet and is located at: <http://gts.honeywell.com/ss>

- Incident response procedure ([See Computer Security Incident Reporting process- Supplied Link](#))

Appendix A – Supporting Policy and Standards

Honeywell Policy & Standards	Content Owner	Honeywell Intranet Location
VPN Policy and Standards	GTS Product Management	http://gsp.honeywell.com/lib/security
Acceptable Use Policy	GTS Security	http://gsp.honeywell.com/lib/security
Honeywell Information Systems Security Policy and Standards	GTS Security	http://gsp.honeywell.com/lib/security
Secure Operating Systems Configurations	GTS Security	http://gsp.honeywell.com/sc
Security Policy Exceptions Process	GTS Security	http://gsp.honeywell.com/lib/security
Web Infrastructure Standards	GTS Delivery Assurance	http://gsp.honeywell.com/lib/infrastructure
Networking Standards	GTS Delivery Assurance	http://gsp.honeywell.com/lib/infrastructure
Honeywell Data Retention Policy	Corporate	http://my.honeywell.com/c2kbeans/docs/7279/RetentionGuidelinesVer2.pdf
Data Classification Policy	Corporate	http://finance.honeywell.com/controllers/policy/pm405.htm

Appendix B - Definitions

Business Connectivity - For secure Business to Business (B2B), or Customer (B2C), and connections with 3rd Parties (non-Honeywell) for fulfilling vendor relationship contractual obligations, privacy controls, and including connections supporting Mergers, Acquisitions and Divestiture actions not explicitly covered by any of the other definitions for connection types where the following connectivity definitions do not apply.

DMZ - Demilitarized Zones, For example, a web DMZ is a zone that is used to terminate connections coming from the internet or an application DMZ is a zone that is used to host application servers for the business logic behind the hosted web services for intranet, extranet, or internet web applications.

DNS – Domain Name Service used in the identification and registration of defined systems within a network to their Internet address space name.

Extranet - Physical connections to vendors, business partners, customers, and non-trusted portions of the Honeywell EWN. Also for physical connections to companies being acquired or divested between the start of the process and either the full network integration or the termination of network connectivity.

FTP – File Transfer Protocol for Internet enabled systems

FWRR - Firewall Rule Request process supported by Global IT Security to facilitate firewall rule management for Honeywell.

GSSA – Global IT Security and Systems Assurance

Highly Sensitive Connections - For DOD and other government locations where compliance is based on legislated obligation to defense and military regulations.

Internet - The public, untrusted internet.

Intranet - The trusted portion of the Honeywell Enterprise Wide Network.

ITG – Information Technology Group, of Honeywell Global Business Services division.

Network Gateways - A controlled, engineered network connection solution designed to facilitate the transmission of multi-protocol communications that connects Honeywell directly or indirectly to the Internet or other non-trusted networks. Any data flow between Honeywell and non-Honeywell networks via the following

Public Connections - Connections to Internet Service Providers or other untrusted networks whether publicly accessible or not that do not belong to a vendor, customer, business partner or the corporation itself.

Remote Access Connections - Providing secure remote access to Honeywell networks singularly for individual users or in groups of Honeywell or non-Honeywell personnel.

SLA – Service Level Agreement

SMTP – Simple Mail Transfer Protocol for Internet based mail services

VPN - Virtual Private Network providing remote access to Honeywell networks using a secure tunneling technology between the remote user client and host Honeywell network.

Zones of Trust - An engineered zone of trust interacts between two networks with different trust levels. These facilitate the secure placement of application hosting servers and Internet services hosting systems adjacent the Internet or within the Honeywell Intranet.