DATA PROCUREMENT DOCUMENT	
NO.	ISSUE
1916	**RFP**

80MSFC26R0006

CONTRACT/RFP

EXHIBIT NUMBER

B

ATTACHMENT NUMBER

Next Extension for User Continuity and Sustainability (NEXUS)

PROJECT/SYSTEM

DATA PROCUREMENT DOCUMENT

Contractor

CONTRACTOR

June 22, 2026

DATE

National Aeronautics and
Space Administration

National Aeronautics and Space Administration ***DOCUMENT CHANGE LOG***					DATA PROCUREMENT DOCUMENT NO. ISSUE **1916 RFP**
INCORPORATED REVISIONS OUTSTANDING REVISIONS				AS OF: 06-11-26	SUPERSEDING: / PAGE: Page 1 of 1
AUTHORITY	PORTION AFFECTED - PAGE NO./NO.				REMARKS
(DPD Revision)	INTRO	SGR	DRL	DRD	
Amendment 01					Revised Data Requirements List for DRD-007.
Amendment 01				008	Revised content of DRD-008.

1.0 INTRODUCTION

1.1 Scope: Subject to the Rights in Data clause, this Data Procurement Document (DPD) sets forth the data requirements in each Data Requirements Description (DRD) and shall govern that data required by the DPD for the contract. The contractor shall furnish data defined by the DRDs listed on the Data Requirements List (DRL) by category of data, attached hereto, and made a part of this DPD. Such data shall be prepared, maintained, and delivered to NASA in accordance with the requirements set forth within this DPD. In cases where data requirements are covered by a Federal Acquisition Regulation (FAR) or NASA FAR Supplement (NFS) clause, that clause shall take precedence over the DPD, consistent with clause FAR 52.215-8, Order of Precedence - Uniform Contract Format *(DEVIATION NOV 2025)*

1.2 DPD Description: This DPD consists of a Document Change Log, an Introduction, a Statement of General Requirements, DPD maintenance procedures, a DRL, and the DRDs.

1.2.1 General Requirements: The general requirements, as specified in paragraph 2.0 of this DPD, prescribe those requirements applicable to the preparation, maintenance, and delivery of data that are better defined in aggregate than in the individual DRDs.

1.2.2 Data Requirements List (DRL): Throughout the performance of the contract, the DRL provides a listing by data category of the data requirements of the DPD.

1.2.3 Data Requirements Description (DRD)

1.2.3.1 Each data requirement listed on the DRL is given complete definition by a DRD. The DRD prescribes content, format, maintenance instructions, and submittal requirements.

1.2.3.2 RESERVED

1.2.3.3 The symbols representing these data categories form part of the prefix of the DRD identification number. The first numerical characters reflect the DPD number.

1.2.3.4 To facilitate the usage and maintenance of the DPD, the DRDs have been sectionalized in accordance with the above data categories.

1.2.3.5 The DRDs are filed by data category and are in alpha-numeric sequence as listed on the DRL page (or pages) that precedes the DRDs.

1.2.4 Document Change Log (DCL): The Document Change Log chronologically records all revision actions that pertain to the DPD.

1.2.5 DPD Maintenance Procedures: Maintenance procedures define the detailed methods to be employed in maintaining the DPD. Detailed maintenance procedures are specified in paragraph 3.0 of this DPD.

1.3 Data Types for Contractual Efforts: The types of data and their contractually applicable requirements for approval and delivery are:

TYPE	DESCRIPTION
1*	All issues and interim changes to those issues require written approval from the requiring organization before formal release for use or implementation.
2*	NASA reserves a time-limited right to disapprove in writing any issues and interim changes to those issues. The contractor shall submit the required data to NASA for review not less than 45 calendar days** prior to its release for use. The contractor shall clearly identify the release target date in the "submitted for review" transmittal***. If the data is unacceptable, NASA will notify the contractor within 45 calendar days** from the date of submission, regardless of the intended release date***. The contractor shall resubmit the information for reevaluation if disapproved. The submittal is considered approved if the contractor does not receive disapproval or an extension request from NASA within 45 calendar days**.
3	These data shall be delivered by the contractor as required by the contract and do not require NASA approval. However, to be a satisfactory delivery, the data shall satisfy all applicable contractual requirements and be submitted on time.
4	These data are produced or used during performance of the contract and are retained by the contractor. They shall be delivered only when NASA requests in writing and shall be delivered in accordance with the instructions in the request. The contractor shall maintain a list of these data and shall furnish copies of the list to NASA when requested to do so.
5	These data are incidental to contract performance and are retained by the contractor in those cases where contracting parties have agreed that formal delivery is not required. However, the Contracting Officer (CO) or the Contracting Officer's Representative (COR) shall have access to and can inspect this data at its location in the contractor's or subcontractor's facilities, or in an electronic database accessible to the Government.

* Note: Type 1 and Type 2 data may be placed under NASA configuration management control when designated by NASA. CM control requires the contractor to submit Type 1 and Type 2 data updates through Engineering Change Proposals (ECPs).

** Note: This time limit may be tailored for individual DRDs to meet the requirements of the procuring activity.

*** Note: If the contractor does not identify a release target date or if the intended release date is shorter than 45 calendar days from the date of submission, the 45 calendar days review cycle stands (or the tailored Type 2 time limitation for the specific procurement).

2.0 STATEMENT OF GENERAL REQUIREMENTS

2.1 Applicable/Reference Documents: Documents included as applicable documents in this DPD are the issue specified in the Statement of Work and form a part of the DPD to the extent specified herein. Applicable documents listed in Item 15.2 of a DRD are applicable only to the preparation of the deliverable documentation described by that DRD.

References to documents other than applicable documents in the data requirements of this DPD may sometimes be utilized and shall be indicated in 13. Remarks of the DRD. These do not constitute a contractual obligation on the contractor. They are to be used only as a possible example or to provide related information to assist the contractor in developing a response to that particular data requirement.

2.2 Subcontractor Data Requirements

2.2.1 The contractor shall specify to subcontractors and vendors, if any, the availability source of all data required for the satisfactory accomplishment of their contracts. The contractor shall validate these requirements for documents when appropriate; where the requirement concerns other contractor data, the contractor shall provide his subcontractor or vendor with the necessary documents. All such requests shall be accomplished under the auspices of the contractor.

2.2.2 Reference to subcontractor data in the contractor's responses is permissible, providing the references are adequate and includes such identification elements as title, number, revision, etc., and a copy of the referenced data is supplied with the response document at time of delivery to NASA.

2.3 Data Distribution, Format, Data Restriction Marking, and Transmittal

2.3.1 Distribution: Distribution of required documentation shall be in quantities determined by the CO. Recipient names and email addresses (if applicable) shall be noted on a separate distribution list to be furnished by the CO. The CO's letter may include other information pertinent to delivery of data, as required.

2.3.2 Format

2.3.2.1 Electronic Format: Electronic submission of data deliverables is required. Electronic deliverables shall be printable. Data deliverables shall be delivered to NASA in the format specified below unless a specific format is required by a DRD. Data submittals shall consist of a single Adobe Acrobat PDF file and the native format electronic file(s). The preferred native formats include Microsoft Word, Excel, PowerPoint or CAD drawing plot file, as appropriate. Where a single native format file is not possible, multiple files may be integrated into a single ZIP file for submission. The organization of the contents of the integrated ZIP file shall be made readily apparent to the reader, and each file within the integrated product shall be clearly identifiable and traceable within the organization of the integrated product. If files are fragmented, file names shall be labeled logically and contiguously, and the files shall be easily reassembled or merged (e.g. 1 filename, 2 filename, 2a filename, etc.). The software versions shall be confirmed prior to submittals.

2.3.2.2 Hardcopy Format: Hardcopy of the DPD is not required unless electronic delivery is not possible or practical. The contractor's transmittal memo shall be delivered in a hardcopy to the CO. The DPD shall be emailed to the CO.

2.3.3 Controlled Unclassified Information (CUI) Data Restriction Markings

2.3.3.1 CUI Data Restriction Determination and Marking Requirements: The contractor shall determine whether each data deliverable contains Controlled Unclassified Information (CUI), information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. Data deliverables that contain CUI shall be managed, marked, and protected in accordance with NPR 2810.7 and CFR 32 Part 2002. Per NPR 2810.7, CUI data shall be marked with a CUI Banner on each page that is inclusive of all CUI within the data. The CUI Banner will be the same on each page, be placed at the top of each page, centered, bolded, in a single line with multiple CUI markings in alphabetic order separated by a single slash (NOTE: See NPR 2810.7 for CUI Specified correct slash and dash placement and usage). In addition, the following statement from Standard Form (SF) 901 may be placed on the title page:

"ATTENTION: This document is CONTROLLED UNCLASSIFIED INFORMATION (CUI). All individuals handling this information are required to protect it from unauthorized disclosure. Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy. Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies."

2.3.3.2 Data Restriction Categories and Marking Statements: In addition to CUI markings, the contractor shall consider the following data restriction categories, as a minimum, and utilize specified marking statements.

2.3.3.2.1 Export Control Restrictions. If data delivered under this contract is subject to export control restrictions, which includes International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR), the export-controlled information is required to be marked "CUI//SP-EXPT" in accordance with NPR 2810.7 prior to dissemination to NASA. CUI//SP-EXPT controlled information is unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives.

If data delivered under this contract is subject to ITAR, in addition to the CUI marking the data shall contain an "ITAR Notice" on the cover page as required by NAII 2190.1, section 2.2.1.1, with the appropriate United States Munitions List (USML) category filled in at the top of the ITAR Notice. On subsequent pages, it is recommended to place the following statement at the bottom or footer, "See title page for restrictions".

USML Category ___
International Traffic in Arms Regulations (ITAR) Notice
This document contains information which falls under the purview of the U.S. Munitions List (USML), as defined in the International Traffic in Arms Regulations (ITAR), 22 CFR §120-130, and is export controlled. It shall not be transferred to foreign persons, in the U.S. or abroad, without specific approval of a knowledgeable NASA export control official, and/or unless an export license or license exemption is obtained/available from the Directorate of Defense Trade Controls, United States Department of State. Violations of these regulations are punishable by fine, imprisonment, or both.

If data delivered under this contract is subject to EAR, in addition to the CUI marking the data shall contain the "EAR Notice" on the cover page as required by NAII 2190.1, section 2.2.1.1, with the appropriate Commerce Control List (CCL) Export Control Classification Number (ECCN) filled in at the top of the EAR Notice. On subsequent pages, it is recommended to place the following statement at the bottom or footer, "See title page for restrictions".

CCL ECCN ___
Export Administration Regulations (EAR) Notice
This document contains information within the purview of the Export Administration Regulations (EAR), 15 CFR §730-774, and is export controlled. It may not be transferred to foreign persons in the U.S. or abroad without specific approval of a knowledgeable NASA export control official, and/or unless an export license or license exception is obtained/available from the Bureau of Industry and Security, United States Department of Commerce. Violations of these regulations are punishable by fine, imprisonment, or both.

2.3.3.2.2 Limited Rights Restrictions. If the contract contains FAR 52.227-14 *Alternate II*, the "Limited Rights Notice" may be applicable to technical data (other than computer software) delivered under this contract. The "Limited Rights Notice" is as follows:

Limited Rights Notice (Dec 2007)
a) These data are submitted with limited rights under Government Contract No. _____ (and subcontract _____, if appropriate). These data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture nor disclosed outside the Government; except that the Government may disclose these data outside the Government for the following purposes, if any; provided that the Government makes such disclosure subject to prohibition against further use and disclosure: [*Agencies may list additional purposes as set forth in* 27.404-2*(c)(1) or if none, so state.* (b) This notice shall be marked on any reproduction of these data, in whole or in part.

2.3.3.2.3 Restricted Rights Computer Software. If the contract contains FAR 52.227-14 *Alternate III*, the "Restricted Rights Notice" may be applicable to computer software delivered under this contract. The "Restricted Rights Notice" is as follows:

Restricted Rights Notice (Dec 2007)
(a) This computer software is submitted with restricted rights under Government Contract No. _____ (and subcontract _____, if appropriate). It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this notice or as otherwise expressly stated in the contract. (b) This computer software may be— (1) Used or copied for use with the computer(s) for which it was acquired, including use at any Government installation to which the computer(s) may be transferred; (2) Used or copied for use with a backup computer if any computer for which it was acquired is inoperative; (3) Reproduced for safekeeping (archives) or backup purposes; (4) Modified, adapted, or combined with other computer software, *provided* that the modified, adapted, or combined portions of the derivative software incorporating any of the delivered, restricted computer software shall be subject to the same restricted rights; (5) Disclosed to and reproduced for use by support service Contractors or their subcontractors in accordance with paragraphs (b)(1) through (4) of this notice; and (6) Used or copied for use with a replacement computer. (c) Notwithstanding the foregoing, if this computer software is copyrighted computer software, it is licensed to the Government with the minimum rights set forth in paragraph (b) of this notice. (d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract. (e) This notice shall be marked on any reproduction of this computer software, in whole or in part.

2.3.3.2.4 Small Business Innovation Research (SBIR) Rights. If the contract contains FAR 52.227-20, the "SBIR Rights Notice" may be applicable to SBIR data delivered under this contract. The "SBIR Rights Notice" is as follows:

SBIR Rights Notice (DEC 2007)
These SBIR data are furnished with SBIR rights under Contract No._____ (and subcontract _____, if appropriate). For a period of 4 years, unless extended in accordance with FAR 27.409(h), after acceptance of all items to be delivered under this contract, the Government will use these data for Government purposes only, and they shall not be disclosed outside the Government (including disclosure for procurement purposes) during such period without permission of the Contractor, except that, subject to the foregoing use and disclosure prohibitions, these data may be disclosed for use by support Contractors. After the protection period, the Government has a paid-up license to use, and to authorize others to use on its behalf, these data for Government purposes, but is relieved of all disclosure prohibitions and assumes no liability for unauthorized use of these data by third parties. This notice shall be affixed to any reproductions of these data, in whole or in part.

2.3.3.2.5 Other Restrictions. If the contract contains NFS 1852.237-73, a sensitive information legend may be applicable to information (which does not qualify as technical data or computer software) delivered under this contract.

In accordance with the applicable data clause (e.g., FAR 52.227-14(c) or FAR 52.227-20(c)), the contractor may be able to assert copyright in data first produced in the performance of the contract. When claim to copyright is made, the Contractor shall affix

the applicable copyright notices of 17 U.S.C. 401 or 402 and acknowledgment of Government sponsorship (including contract number) to the data.

2.3.4 Transmittal

2.3.4.1 Data shall be transmitted to NASA by email, CD or DVD, hardcopy, or other mechanism agreed to by the CO, COR, and Project representatives who are responsible to receive, index, and store the data deliverables.

2.3.4.2 If email is used to transmit data deliverables, the email size shall be 10 Megabytes or less to ensure receipt by the NASA email servers. Encrypted email format shall be used to transmit data which has been judged sensitive by the contractor (e.g., export controlled, limited rights data, SBIR, restricted computer software, copyrighted, etc.).

2.3.4.3 Data Transmittal Package: Each data transmittal package shall include:

a. Transmittal memorandum that specifies the meta-data below for each data transmittal:
   1. Contract number.
   2. Data Requirements Description (DRD) number.
   3. DRD data type (specified in Item 3 on the DRD).
   4. Submission date or milestone being satisfied.
   5. Document number and revision.
   6. Document title.
   7. File names of all files being delivered; file naming convention shall clearly identify the document being delivered.
   8. Distribution (as defined by the CO's letter).
   9. Requested response date.
   10. Contractor assigned data restriction (export controlled, limited rights data, SBIR, restricted computer software, copyrighted, etc.) if not marked on data.
   11. NASA Records Retention Schedule (NRRS) number, if applicable (See NRRS 1441.1, NASA Records Retention Schedules).
b. Printable electronic files or hardcopy data.

2.3.5 When electronic data deliverables are transmitted directly to the MSFC Repository, SharePoint web interface shall be utilized. Instructions for electronic data submittals can be found at https://sharepoint.msfc.nasa.gov/rm/repo/SitePages/Home.aspx. For further information, contact the MSFC Repository Manager.

2.4 Printing: All printing, duplicating, or binding shall be in accordance with NFS 1852.208-81 (*DEVIATION PCD 25-18*), Restrictions on Printing and Duplicating. Printing formal reports and Type 1 and 2 data in book format shall be in accordance with the following general specifications:

a. Method of reproduction – offset/xerography.
b. Finished size – 8 1/2" X 11".
c. Paper – 20-pound opaque bond.
d. Cover – Litho cover stock.
e. Pages shall be printed on both sides; blank pages shall be avoided when possible.
f. Oversize pages shall be avoided, when possible, but, if necessary, shall be folded to 8 1/2" X 11".

g. Binding shall be the most economical method commensurate with the size of the report and its intended use.

2.5 Contractor's Internal Documents: The contractor's internal documents shall be used to meet the data requirements of this DPD unless a specific format is required by the applicable DRD.

2.6 Document Identification: Type 1 and 2 documents published by the contractor and submitted in response to the data requirements of this DPD shall be identified within an organized identification numbering system prescribed to NASA by the contractor and, if applicable, as approved by NASA. For all data types, the document number, change legend, date, and title constitute the minimum identification of the specific document and shall appear on the cover and title page. The contract number shall also appear on the cover and title page as separate markings. The originator and organization shall be included on the title page. The document number, change legend, and date shall appear on each page of the document. In the front matter of each document, identify the DPD number and applicable DRD number(s) required for document preparation. Successive issues or revisions of documents shall be identified in the same manner as the basic issue and shall have appropriate change identification. Drawings and ECP's are excluded from the marking provisions of this paragraph. All Type 1 documentation, excluding configuration management requirements, shall be marked "PRELIMINARY PENDING NASA APPROVAL," and once approved shall be reissued with "APPROVED BY NASA" and the date and approval authority annotated on the cover.

2.7 Reference to Other Documents and Data Deliverables in Data Submittals: All referenced documents shall be made readily available to the cognizant NASA organization upon request. The contractor shall make sure that the references are available to NASA in a manner which does not incur delays in the use of the response document. Reference may be made, within one data submittal, to other data submittals delivered in response to this DPD in those cases where the data required by one DRD may have been delivered by the contractor in response to another DRD. The reference to previously submitted data shall include the applicable DRD number, data submittal version date, and location within the referenced document.

2.8 Maintenance of Type 1 Document Submittals

2.8.1 Revisions of Type 1 documentation may be accomplished either by individual page revision or by a complete reissue of the document identified in accordance with requirements of 2.6 above, with the exception of drawings (which shall be revised in accordance with contract configuration management requirements).

2.8.2 Individual page revisions shall be made as deemed necessary by the contractor or as directed by the CO.

2.8.3 A Type 1 document shall be completely reissued when, in the opinion of the contractor and/or NASA, the document has been revised to the extent that it is unusable in its present state, or when directed by the CO. When complete reissues are made, the entire contents of the document shall be brought up to date and shall incorporate revised pages. All revisions

shall be recorded. A revision log shall identify complete reissues except for periodic reports and documents which are complete within themselves as final.

2.8.4 Changes of a minor nature to correct obvious typing errors, misspelled words, etc., shall only be made when a technical change is made, unless the accuracy of the document is affected.

2.8.5 All revised pages shall be identified by a revision symbol and a new date. Each document shall contain a log of revised pages that identify the revision status of each page with the revision symbol. This list shall follow the table of contents in each document. The line or lines revised on a given page shall be designated by the use of vertical line in the margin of the page, and the change authority shall be indicated adjacent to the change.

2.8.6 Contractor Type 1 document shall not be submitted containing pen and ink markups which correct, add to, or change the text, unless schedule problems exist and approval is obtained in writing from the CO. Such markups, however, shall not exceed 20 percent of the page content and shall be acceptable provided that the reproduced copies are legible. In addition, hand-drawn schematics, block diagrams, data curves, and similar charts may be used in original reports in lieu of formally prepared artwork, as long as legibility of copies is not impaired. Acceptability shall be determined by the CO.

3.0 DPD MAINTENANCE PROCEDURES

3.1 NASA-Initiated Change: New and/or revised data requirements shall be incorporated by contract modification to which the new or revised portion of the DPD shall be appended. The contractor shall notify the CO in the event a deliverable data requirement is imposed and is not covered by a DRD, or when a DRD is changed by a contract modification and for which no revision to DPD is appended. In such cases, the contractor shall submit the requested changes to NASA for approval. See paragraph 3.3.1 for change procedures.

3.2 Contractor-Initiated Change: Contractor-proposed data requirements or proposed changes to existing requirements shall be submitted to NASA for approval.

3.3 DPD Change Procedures

3.3.1 Changes to a contractual issue of this DPD shall be identified by NASA on the Document Change Log.

3.3.2 The date of the DPD shall be entered under the “as of” block of the Document Change Log. The date that was in the “as of” block shall be entered in the “Superseding” block.

3.3.3 The Document Change Log entitled “Incorporated Revisions” shall be changed to indicate the modification number, portions affected, and remarks. All changes to the DPD/DRDs shall be identified in the “Remarks” column.

3.4 DPD Reissues

3.4.1 When conditions warrant, the DPD shall be reissued by NASA for each contract modification that affects the DPD and shall supersede the existing DPD in its entirety. Reissues shall be issued by contractual direction.

3.4.2 All revision dates shall remain in the Date Revised block on all DRDs. The issue symbol, which shall commence with "A" and progress through "Z," shall be entered in the DPD identification block of each DRD page of the DPD.

3.5 Contract Line-Item Number: A uniquely numbered contract item used to identify and manage specific deliverables, services, work scope, or funding elements within a Government contract. CLINs establish the contractual basis for performance, pricing, funding, and payment.

3.6 Authority to Proceed (ATP): A formal Government authorization that allows a contractor to begin a specified phase of contract work, incur associated costs, and execute activities defined within the contract or task order. ATP is typically issued after the Government determines that required prerequisites, approvals, funding, and readiness criteria have been satisfied.

Next Extension for User Continuity and Sustainability (NEXUS)

Data Requirements List (DRL)

DRD	DATA TYPE	TITLE	OPR
NEXUS-DRD-001	1	Service Requirements Compliance Matrix (SRCM)	NEXUS
NEXUS-DRD-002	1	Service Demonstration & Validation Plan (SDVP)	NEXUS
NEXUS-DRD-003	1	Verification Closure Notices (VCN)	NEXUS
NEXUS-DRD-004	2	External Interface Control Documents (ICDs)	NEXUS
NEXUS-DRD-005	2	Security Architecture Definition (SAD)	NEXUS
NEXUS-DRD-006	2	Service Transition Plan (STP)	NEXUS
NEXUS-DRD-007	2	Intellectual Property & Data Rights Management Plan (IPDRMP)	NEXUS
NEXUS-DRD-008	1	Service Financial & Pricing Structure Definitions (SFPSD)	NEXUS
NEXUS-DRD-009	2	Training Emulator	NEXUS
NEXUS-DRD-010	3	Continuity of Service Operations Plan (CSOP)	NEXUS
NEXUS-DRD-011	2	Verification/Validation Compliance Report (VVCR)	NEXUS
NEXUS-DRD-012	1	CLIN 1 Decision Report and Presentation Package	NEXUS
NEXUS-DRD-013	1	CLIN 2 Demonstration Readiness Package	NEXUS
NEXUS-DRD-014	2	Monthly Program Status Report (MPSR)	NEXUS
NEXUS-DRD-015	2	CLIN 2 Demonstration Performance Validation Package (DPVP)	NEXUS
NEXUS-DRD-016	1	Organizational Conflict of Interest (OCI) Plan	OP
NEXUS-DRD-017	1	Security Requirements for Unclassified IT Resources	OCIO
NEXUS-DRD-018	1	Demonstration Integration & Maturity Presentation Package	NEXUS
NEXUS-DRD-019	2	Integrated Master Schedule (IMS)	NEXUS
NEXUS-DRD-020	2	Radio Frequency Link Margin and Dynamic Link Budget Analysis Report (RF-LMDBAR)	NEXUS

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: NEXUS **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-001**
3. **DATA TYPE**: 1
4. **DATE REVISED**:
5. **PAGE**: 1/2

6. **TITLE**: Service Requirements Compliance Matrix (SRCM)

7. **DESCRIPTION/USE**: Provides compliance with the NEXUS Service Requirements Document (SRD) to include expected compliance, compliance rationale, verification approach, and verification evidence, along with references to any analysis, test, or other substantiating evidence used to demonstrate compliance. Enables the Government to verify compliance with NASA-provided service requirements and assess the Contractor's approach to meeting requirements during the Demonstration Phase.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief:** Not applicable; **CLIN 2 Authorization to Proceed (ATP) + 30 days**: Initial Baseline. **Demonstration & Integration Maturity Checkpoint**: Final Baseline. **Demonstration Readiness Review**: Update compliance matrix as required. **Demonstration Performance Validation Review**: Update compliance matrix as required.

12. **SUBMISSION FREQUENCY**: Update as required or upon significant changes to requirements verification approach

13. **REMARKS**: This DRD supports the Government's need to evaluate progress toward demonstration objectives and support formal milestone reviews. The Service Requirements Compliance Matrix is a Type 1 data item requiring formal Government review and approval.

14. **INTERRELATIONSHIP**: NEXUS-DRD-002, Service Demonstration & Validation Plan, NEXUS-DRD-003, Verification Closure Notices and applicable contract paragraphs [TBD] related to verification and compliance demonstration.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The Service Requirements Compliance Matrix (SRCM) provides comprehensive traceability from each NEXUS Service Requirements Document (SRD) requirement to the verification method(s) and evidence used to demonstrate compliance. The SRCM serves as the primary document for demonstrating how the Contractor's service architecture, implementation, and performance meet NASA service requirements. This document enables objective performance verification and supports informed transition decisions from Demonstration.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:

NEXUS-RQMT-001 *NEXUS Service Requirements Document (SRD)*

DRD Continuation Sheet

TITLE: Service Requirements Compliance Matrix (SRCM) **DRD NO.**: **NEXUS-DRD-001**
DATA TYPE: 1 **PAGE**: 2/2

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

15.3 **CONTENTS**: The Service Requirements Compliance Matrix (SRCM) must include the following:

a. Complete listing of all NEXUS SRD requirements with unique requirement identifiers.
b. Traceability mapping from NEXUS SRD requirements to first-level Contractor derived/decomposed requirements and associated verification method(s) to be employed (e.g., test, analysis, inspection, demonstration).
c. Verification compliance rationale for each NEXUS SRD requirement, including:
    1. Description of the verification approach.
    2. Status of verification (planned, in-progress, complete).
    3. Compliance determination (compliant, non-compliant, partially compliant, not yet verified).
d. References and access to substantiating evidence including:
    1. Test reports and results.
    2. Analysis documentation.
    3. Inspection records.
    4. Demonstration data.
    5. Other relevant verification artifacts.
e. Documentation of any deviations, waivers, or variances from stated requirements, including proposed mitigation approaches.
f. Cross references to related verification documentation including the Service Demonstration & Validation Plan and Verification Closure Notices.
g. Explicit identification of verification and validation evidence derived from end-to-end service demonstration, including:
    1. Mapping of demonstration scenarios to SRD requirements.
    2. Identification of multi-user, high-load, and stressed condition validation cases.
    3. Traceability to NEXUS-DRD-002, Service Demonstration and Validation Plan activities.

15.4 **FORMAT**: Contractor format is acceptable. The matrix may be provided in spreadsheet, database, or other electronic format that supports sorting, filtering, and traceability analysis. At a minimum, the following fields should be included: Requirement ID, Requirement Text, Verification Method, Verification Status, Compliance Status, Rationale, and Evidence References.

15.5 **MAINTENANCE**: The SRCM must be maintained current throughout the Demonstration Phase. Changes and/or updates must be submitted in accordance with the schedule specified in Item 12 or as requested by the Government. Updates must reflect changes in requirements, verification approaches, verification status, and compliance determinations. The Contractor must highlight all changes from the previous submission and provide a summary of significant updates in a transmittal letter or revision history section. Changes and/or updates must be in accordance with the provider/contractor's approved change control system.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: NEXUS **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-002**
3. **DATA TYPE**: 1
4. **DATE REVISED**:
5. **PAGE**: 1/4

6. **TITLE**: Service Demonstration & Validation Plan (SDVP)

7. **DESCRIPTION/USE**: To define the test approach, requirement validation matrix mapping validation tests to requirements with associated validation criteria, and demonstration acceptance thresholds for the NEXUS service. This plan documents the validation activities and organizational structure necessary to demonstrate performance against NASA service requirements.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief:** Not applicable; **CLIN 2 Authorization to Proceed (ATP) + 30 days**: Initial Baseline; **Demonstration & Integration Maturity**: Final Baseline; **Demonstration Readiness Review**: Update as required or upon significant changes to requirements validation approach; Demonstration **Performance Validation Review**: Update as required.

12. **SUBMISSION FREQUENCY**: Update as required or prior to major validation activities

13. **REMARKS**: This DRD supports the Government's need to evaluate progress toward demonstration objectives and enable objective performance verification as identified in Attachment E of the Government Insight Deliverables document. The Service Demonstration & Validation Plan is a Type 1 data item requiring formal Government review and approval. This plan may be supplemented by specific test procedures, analysis plans, or demonstration scripts as appropriate, provided the collective documentation meets the content requirements specified herein.

14. **INTERRELATIONSHIP**: NEXUS-DRD-001, Service Requirements Compliance Matrix, NEXUS-DRD-003, Verification Closure Notices and NEXUS-DRD-004, External Interface Control Documents and applicable contract paragraphs [TBD] related to verification and compliance demonstration.

DRD Continuation Sheet

TITLE: Service Demonstration & Validation Plan (SDVP) **DRD NO.**: **NEXUS-DRD-002**
DATA TYPE: 1 **PAGE**: 2/4

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The Service Demonstration & Validation Plan (SDVP) provides a comprehensive description of the Contractor's approach to validating service performance during the Demonstration Phase. The plan defines the strategy, methods, criteria, and acceptance thresholds for demonstrating that the NEXUS service meets NASA-provided service requirements at the defined demarcation boundaries. The validation approach must include end-to-end validation across the complete service chain from user system interfaces through the space relay and ground segments and return path, including representative or actual user systems. This document addresses validation of service architecture, interfaces, performance parameters, and operational capabilities necessary to support informed relay service transition decisions. The SDVP emphasizes demonstrated outcomes and objective performance verification while preserving Contractor flexibility in design and implementation approach.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:
NEXUS-RQMT-001 *NEXUS Service Requirements Document (SRD)*

15.3 **CONTENTS**: The Service Demonstration & Validation Plan (SDVP) must include the following:

a. Overview of the service demonstration and validation program, including:
   1. Validation philosophy and approach.
   2. Demonstration phase objectives and success criteria.
   3. Relationship to Initial Operational Capability (IOC) readiness determination.
   4. Schedule and phasing of validation activities.
b. Requirement Validation Matrix that maps each NEXUS SRD requirement to planned validation test(s), including:
   1. Requirement identifier and text.
   2. Validation method (test, demonstration, analysis, inspection).
   3. Validation test identifier and description.
   4. Associated validation criteria (pass/fail criteria, measurement parameters).
   5. Demonstration acceptance thresholds (quantitative performance thresholds).
   6. Planned validation timeline.
c. Detailed test approach and methodology, including:
   1. Test architecture and configuration.
   2. Test scenarios and use cases.
   3. Test procedures and protocols.
   4. Data collection and measurement methods.
   5. Test environment description (facilities, equipment, simulators).
   6. End-to-end validation architecture including user system participation and full-service path representation.
d. Description of the organizational structure for implementing the validation program, including:
   1. Organizations involved in validation activities.
   2. Roles and responsibilities for test execution, data collection, and analysis.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:
    3. Review and approval authority for validation results.
    4. Interface with Government oversight and observation activities.

e. Detailed descriptions of all planned validation activities including:
    1. Prerequisites, dependencies, and constraints including spectrum authorization for RF testing.
    2. Objectives and expected outcomes.
    3. Success criteria and acceptance thresholds.
    4. Risk mitigation strategies.
    5. Contingency plans for test anomalies or failures.
    6. Validation under multi-user access scenarios.
    7. Validation under high-load or stressed service conditions.
    8. Validation of degraded or constrained operational modes.

f. Time-correlated sequence of validation activities, including:
    1. Validation activity schedule with key milestones.
    2. Dependencies between validation events.
    3. Integration with overall demonstration phase schedule.
    4. Government observation or participation opportunities.

g. Description of the validation environment and supporting capabilities sufficient to demonstrate credible execution of verification and validation activities, including:
    1. The overall validation architecture and approach (e.g., test, analysis, demonstration, simulation).
    2. High-level description of representative validation assets (e.g., test environments, instrumentation, or tools), to the extent necessary to demonstrate adequacy and credibility of the validation approach, without requiring disclosure of proprietary implementation details.
    3. Capabilities supporting interface validation and interoperability validation at defined service demarcation boundaries for ground and space segments used to exercise end-to-end service performance.
    4. Modeling, simulation, or emulation capabilities used to supplement validation, including their role and limitations, data processing, analysis, and evidence generation methods used to support verification closure and Government Inspection of Records (IoR).

h. Data management approach including:
    1. Validation data collection, storage, and access procedures
    2. Test results documentation and reporting.
    3. Traceability to Service Requirements Compliance Matrix.
    4. Evidence package preparation for Verification Closure Notices.

i. Identification of any validation deviations, limitations, or assumptions, including those that may affect end-to-end service performance or multi-user operational behavior

j. Identification of demonstration Test Like You Fly (TLYF) exceptions.

DRD Continuation Sheet

TITLE: Service Demonstration & Validation Plan (SDVP) **DRD NO.**: **NEXUS-DRD-002**
DATA TYPE: 1 **PAGE**: 4/4

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

15.4 **FORMAT**: Contractor format is acceptable. The plan may be organized in sections, chapters, or modules as appropriate to the Contractor's approach. The Requirement Validation Matrix may be provided as an integrated section within the plan or as a separate controlled appendix/annex, and may utilize spreadsheet, database, or other electronic format that supports sorting, filtering, and traceability analysis.

15.5 **MAINTENANCE**: The SDVP must be maintained current throughout the Demonstration Phase. Changes and/or updates shall be submitted in accordance with the schedule specified in Item 12 or as requested by the Government. Updates must reflect changes in requirements, validation approaches, test schedules, validation criteria, acceptance thresholds, or organizational structure. The Contractor must highlight all changes from the previous submission and provide a summary of significant updates in a transmittal letter or revision history section. Changes and/or updates must be in accordance with the provider/contractor's approved change control system.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: NEXUS **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-003**
3. **DATA TYPE**: 1
4. **DATE REVISED**:
5. **PAGE**: 1/3

6. **TITLE**: Verification Closure Notices (VCN)

7. **DESCRIPTION/USE**: To document verification closure statements with rationale for closure of NEXUS service requirements, including references and access to actual verification data. These notices provide formal documentation that individual NASA-provided service requirements or groups of requirements have been successfully verified.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief**: Not applicable; **CLIN 2 Authorization to Proceed + 30 days**: Initial verification closure notices as applicable; **Demonstration & Integration Maturity**: Updated verification closure notices as applicable; **Demonstration Readiness Review**: Compilation of VCNs for all verified requirements; apart from those requirements with Demo flight verification test activities planned for requirement closure; **Demonstration Performance Validation Review**: Final compilation of VCNs for all NEXUS service requirements NLT 30-days post demonstration flight tests.

12. **SUBMISSION FREQUENCY**: Submit as verification activities are completed or as requirements are closed.

13. **REMARKS**: MSFC-HDBK-2221 Volume II provides examples of verification closure documentation that can be used as a guide in the development of or in the assessment of similar documentation. This DRD supports the Government's need to verify compliance with NEXUS service requirements and evaluate progress toward demonstration objectives as identified in Attachment C of the Government Insight Deliverables document.

    VCNs are Type 1 data items requiring formal Government review and approval. VCNs may be submitted individually as verification activities are completed or in consolidated packages covering related requirements, provided all required content is included and traceability is maintained.

14. **INTERRELATIONSHIP**: NEXUS-DRD-001, Service Requirements Compliance Matrix, NEXUS-DRD-002, Service Demonstration & Validation Plan and applicable contract paragraphs [TBD] related to verification and compliance demonstration.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The Verification Closure Notices (VCN) provide formal documentation that specific NEXUS Service Requirements Document (SRD) requirements have been successfully verified through completion of planned verification activities. Each VCN documents the verification approach executed, presents the verification evidence and results, provides a rationale for requirement closure, and includes references to the actual verification data packages. VCNs serve as the definitive record demonstrating that individual NEXUS service requirements have been met and support the Government's assessment of Initial Operational Capability (IOC) readiness. The VCNs enable objective performance verification and support Government transition decisions (e.g., Demonstration to IOC) by providing traceable evidence of requirement verification, while also providing Government insight into verification completeness and quality.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:

NEXUS-RQMT-001 *Service Requirements Document (SRD)*

15.3 **CONTENTS**: Each Verification Closure Notice (VCN) must include the following:

a. Requirement identification and traceability information:
   1. Unique requirement identifier(s) from the NEXUS SRD.
   2. Complete requirement statement(s).
   3. Parent/child requirement relationships, if applicable
   4. Cross-reference to Service Requirements Compliance Matrix per NEXUS-DRD-001.

b. Verification summary statement clearly declaring the verification status (e.g., "Requirement XXX has been successfully verified and is recommended for closure").

c. Verification approach and methodology:
   1. Description of verification method(s) employed (test, demonstration, analysis, inspection).
   2. Summary of verification activities performed.
   3. Verification environment and configuration.
   4. Dates of verification activities

d. Verification results and evidence:
   1. Summary of verification data collected.
   2. Test results, measurements, or analysis outputs.
   3. Comparison of actual results against acceptance criteria/thresholds.
   4. Identification of any anomalies, deviations, or non-conformances encountered and their resolution.
   5. Photographic, video, or other documentary evidence as appropriate.
   6. Identification of whether verification evidence includes end-to-end demonstration results and associated operational conditions.

e. Rationale for verification closure, including:
   1. Technical justification that the requirement has been satisfied.
   2. Assessment of verification completeness and adequacy.
   3. Explanation of how verification results demonstrate compliance.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

4. Discussion of any limitations, assumptions, or conditions affecting the verification.
5. Identification of any waivers, deviations, or variances approved

f. References and access to actual verification data:

1 Identification and location of detailed test reports, analysis reports, inspection records, or other verification documentation.
2. Document identifiers, revision levels, and dates.
3. Data repository location or access instructions.
4. List of supporting evidence packages.
5. References to specific sections within larger documents

g. Approval signatures and dates:

1. Contractor verification lead or responsible engineer.
2. Contractor program/project approval authority.
3. Date of closure recommendation

h. Cross-references to related verification activities:

1. Links to Service Demonstration & Validation Plan activities.
2. Dependencies on other requirement verifications.
3. Related Interface Control Document (ICD) verification activities

i. Any supplementary information necessary to support Government review and approval:

1. Lessons learned or observations from verification activities.
2. Identification of follow-on verification activities, if any.
3. Identification of any operational constraints, limitations, or performance sensitivities identified during verification activities

15.4 **FORMAT**: Contractor format is acceptable. VCNs may be submitted as individual documents for each requirement, consolidated documents covering related requirements, or as entries in a verification database or tracking system, provided all required content is accessible and traceable. Each VCN should be uniquely identified and version controlled. Electronic submission with hyperlinks to support evidence packages is encouraged to facilitate Government review and access to actual verification data.

15.5 **MAINTENANCE**: Individual VCNs must be considered final upon Government approval and must not require routine updating. However, if post-closure issues are identified (e.g., verification data errors, requirement changes, operational anomalies), the Contractor must submit revised VCNs with clear identification of changes, rationale for revision, and updated closure justification. A master VCN tracking log must be maintained and updated to reflect submission dates, approval status, and revisions for all VCNs. The tracking log must be submitted monthly or as requested by the Government to provide insight into verification progress and closure status across all NEXUS SRD requirements. Changes and/or updates must be in accordance with the provider/contractor's approved change control system.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: NEXUS **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-004**
3. **DATA TYPE**: 2
4. **DATE REVISED**:
5. **PAGE**: 1/5

6. **TITLE**: External Interface Control Documents (ICDs)

7. **DESCRIPTION/USE**: To document the following for demonstration: 1) Technical characteristics of the RF interfaces between the customer vehicle and the NEXUS relay satellite.; 2) Technical characteristics of the digital IF interfaces between the customer control center/system and the NEXUS ground system; and 3). Characteristics of the external interfaces for the scheduling, configuring, monitoring, and controlling of services by the customer control center/system.

   The External ICDs are intended to define the information exchanges, protocols, interface constraints, and operational interaction mechanisms necessary to enable interoperability and service execution at the NEXUS demarcation boundaries. The ICDs are not intended to provide detailed spacecraft designs, proprietary user system architectures, or complete technical definitions for all individual User missions or satellites. The Contractor should not assume that the Government will provide detailed interface definitions, operational concepts, or technical implementation data for all individual User satellites, spacecraft, or missions. The Contractor's interface approach must accommodate service interaction through standardized or adaptable interface mechanisms consistent with the NEXUS service-based acquisition philosophy

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief**: Not applicable; **CLIN 2 Authorization to Proceed + 30 days**: Initial Baseline; **Demonstration & Integration Maturity**: Final Baseline; **Demonstration Readiness Review**: Update as required; **Demonstration Performance Validation Review**: Update as required

12. **SUBMISSION FREQUENCY**: Update as required or when interface definitions change

13. **REMARKS**: This DRD supports the Government's need to assess technical feasibility and interface interoperability at defined demarcation boundaries as identified in Attachment E of the Government Insight Deliverables document. The Interface Control Documents are Type 2 data items subject to Government review and approval by exception, with a 45-calendar day review period. ICDs may be submitted as individual documents for each major interface or as a consolidated ICD package covering multiple related interfaces, provided all required content is included and interfaces are clearly delineated. The ICDs are critical for validating service architecture and supporting interface verification testing during the Demonstration Phase.

14. **INTERRELATIONSHIP**: NEXUS-DRD-002, Service Demonstration & Validation Plan, NEXUS-DRD-005, Security Architecture Definition, and applicable contract [TBD] paragraphs related to interface requirements and interoperability validation and applicable contract paragraphs [TBD] related to verification and compliance demonstration.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The External Interface Control Documents (ICDs) defines the required content for interface documentation supporting interoperability between the NEXUS service architecture and external entities at defined demarcation boundaries. The scope is limited to information necessary to support service interaction, interoperability, scheduling, configuration, monitoring, and operational coordination. Detailed technical definitions for individual User spacecraft or mission systems are outside the scope of this DRD unless specifically identified by the Government. The Contractor must identify applicable open standards, document any proprietary extensions or constraints, and clearly state assumptions that may affect interoperability, multi-provider integration, or future service expansion.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:
NEXUS-RQMT-001 *Service Requirements Document (SRD)*

15.3 **CONTENTS**: The External Interface Control Documents (ICDs) must include the following content, organized by interface type or as appropriate to the NEXUS service architecture:

a. General Information:
   1. ICD identification, revision level, and date.
   2. Scope and applicability of the ICD.
   3. Interface overview and context diagram.
   4. Description of interfacing systems/entities at the defined service demarcation boundaries (by system class/type, not specific users or missions).
   5. Definition of external service interaction points, service request parameters, operational coordination interfaces, and interoperability constraints necessary to support NEXUS service execution at the defined demarcation boundaries.
   6. Demarcation boundary definition and responsibility allocation.
   7. Identification of applicable interface standards and protocols supporting interoperability, including any deviations or proprietary elements.
   8. Acronyms, abbreviations, and definitions.
   9. Points of contact for interface coordination.

b. Radio Frequency (RF) Interface Characteristics:
   1. Frequency allocations and channel assignments; RF spectrum licensing status.
   2. Polarization characteristics.
   3. Power levels (EIRP, G/T, antenna gain patterns).
   4. Bandwidth and spectral characteristics.
   5. Link budget analysis and margins.
   6. Pointing capabilities and coverage areas.
   7. Doppler considerations.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

8. Interference mitigation, coordination requirements, and operational constraints necessary to maintain service performance in the presence of co-frequency, adjacent-band, or co-located systems.
9. Regulatory compliance information (spectrum licensing).

c. Ground Network Interfaces:

1. Ground interface architecture (Architecture of the digital IF interface between the customer control center/system and NEXUS ground system).
2. Forward Service Digital IF Interface (Characteristics of the digitally sampled Forward Service IF signal provided by the customer control center/system to the NEXUS ground system).
3. Return Service Digital IF Interface (Characteristics of the digitally sampled Return Service IF signal provided by the NEXUS ground system to the customer control center/system).
4. Digital Transport Interface (Transport mechanism used to convey digital IF signals between the customer control center/system and the NEXUS ground system).
5. Timing and Synchronization (Timing and synchronization requirements associated with the digital IF interface).
6. Interface Configuration and Control (Configuration parameters and control information required to establish or modify Forward or Return Service interfaces).
7. Monitoring and Status Information (Interface monitoring information available to the Customer control center).
8. Interface Performance Constraints (Performance constraints applicable to the digital IF interfaces).

d. Application Programming Interface (API):

1. API Overview.
2. API Architecture and Design.
3. API access methods and Authentication.
4. API Reference Documentation.
5. Data Models and Schemas.
6. Data exchange formats between API and other interfaces.
7. Service Request and Provisioning Functions.
8. Scheduling and Reservation Functions (example functions incl., but not limited to, request, modify, prioritize, cancel, and monitor service reservations through provided interfaces)
9. Data Transfer and File Management.
10. Error Handling and Status Codes.
11. Code Examples and SDKs.
12. API Security and Best Practices.
13. Versioning and Backward Compatibility.
14. Monitoring and Status Retrieval.
15. User and Account Management.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:
    16. Testing and Sandbox Environment.
    17. Change Log and Release Notes.
    18. Compliance and Standards.
    19. Support and Resources.

e. User Interaction and Scheduling Interfaces:
    1. User service request procedures and format.
    2. Scheduling request interfaces and protocols

f. Service reservation and allocation mechanisms:
    1. User notification and status reporting interfaces.
    2. Mission planning interface requirements.
    3. Contact scheduling parameters and constraints.
    4. Real-time monitoring and control interfaces.
    5. Post-pass data delivery interfaces and formats.
    6. Customer support and help desk interfaces.

g. Interface Performance and Quality Requirements:
    1. Availability and reliability requirements.
    2. Performance thresholds and acceptance criteria.
    3. Interface monitoring and reporting requirements.
    4. Anomaly reporting and resolution procedures.
    5. Maintenance windows and notification requirements.
    6. Interface performance impacts due to interference, loading conditions, or multi-user access scenarios.

h. Interface Verification and Validation:
    1. Interface verification approach and test methods.
    2. Interoperability test requirements, including validation of compatibility with external or alternate service providers using standards-based interfaces.
    3. Interface validation criteria and acceptance thresholds.
    4. Cross-reference to Service Demonstration & Validation Plan.
    5. Interface compatibility certification procedures.

i. Interface Change Control:
    1. Change management procedures.
    2. Version control and configuration management.
    3. Impact analysis requirements for interface changes.
    4. Notification and coordination procedures.
    5. Backwards compatibility considerations.

j. Operational Constraints and Limitations:
    1. Interface operational constraints.
    2. Environmental constraints affecting interface performance.
    3. Known limitations or conditions.
    4. Contingency operations and degraded mode interfaces.
    5. Failure modes and recovery procedures.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

k. Supporting Information:

1. Interface drawings, diagrams, and schematics.
2. Message catalogs and data dictionaries.
3. Example transactions and use cases.
4. Interface compliance matrices.
5. API Users Guide.

15.4 **FORMAT**: Contractor format is acceptable. ICDs may be organized as individual documents for each major interface category (e.g., separate ICDs for spacecraft interfaces, ground network interfaces, user scheduling interfaces) or as a consolidated ICD document with clearly delineated sections for each interface. Electronic format with searchable content, hyperlinks, and embedded diagrams is preferred. Interface diagrams should follow standard interface definition conventions (e.g., block diagrams, protocol stack diagrams, timing diagrams). Where applicable, industry-standard ICD formats may be utilized.

15.5 **MAINTENANCE**: The ICDs must be maintained current throughout the Demonstration Phase and into operational service delivery. Changes and/or updates must be submitted in accordance with the schedule specified in Item 12, prior to implementing any interface changes, or as requested by the Government. All updates must follow the interface change control procedures defined within the ICDs. Significant interface changes requiring Government review must be submitted at least 30 days prior to planned implementation. The Contractor must highlight all changes from the previous submission using revision marks or a comprehensive revision summary and must provide assessment of impacts on interfacing systems and verification activities. Changes and/or updating must be in accordance with the provider/contractor's approved change control system. ICD revision history must be maintained and included in each submission.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: NEXUS **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-005**
3. **DATA TYPE**: 2
4. **DATE REVISED**:
5. **PAGE**: 1/6

6. **TITLE**: Security Architecture Definition (SAD)

7. **DESCRIPTION/USE**: To define the security architecture design addressing all aspects of cybersecurity, encryption, and other security protocols for the NEXUS service. Includes submittal of a Cybersecurity Assessment and Authorization (CASQ) package. This document enables the Government to assess cybersecurity risks, resolve cybersecurity concerns, protect Government interests during demonstration execution, and ensure compliance with NASA security requirements and policies during the Demonstration Phase.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination; distribution limited based on security classification and sensitivity

11. **SUBMISSIONS**: **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief**: Not applicable; **CLIN 2 Authorization to Proceed + 30 days**: Initial Baseline; **Demonstration & Integration Maturity**: Final Baseline; **Demonstration Readiness Review**: Update as required; **Demonstration Performance Validation Review**: Update as required

12. **SUBMISSION FREQUENCY**: Update as required, when security architecture changes, upon completion of security assessments, or as requested by the Government for cybersecurity risk resolution

13. **REMARKS**: Reference applicable NASA cybersecurity policies, NIST standards (e.g., NIST SP 800-53, NIST Cybersecurity Framework), and Federal Information Security Modernization Act (FISMA) requirements. This DRD supports the Government's need to resolve cybersecurity risks and protect Government interests as identified in Attachment C of the Government Insight Deliverables document. The Security Architecture Definition is a Type 2 data item subject to Government review and approval by exception, with a 45-calendar day review period. It is the Government's intention to reduce duplication of effort by allowing industry to use evidence from other risk frameworks to meet NEXUS requirements. In these cases, crosswalks and gap analysis can be used to leverage existing standard adoption, like ISO 27001, or CMMC2.0 Where appropriate, the Contractor may consolidate cybersecurity and CASQ artifacts to reduce administrative burden while maintaining required insight. Due to the sensitive nature of security information, special handling and distribution restrictions apply to this deliverable.

14. **INTERRELATIONSHIP**: NEXUS-DRD-002, Service Demonstration & Validation Plan, NEXUS-DRD-004, External Interface Control Documents, and applicable contract paragraphs [TBD] related to cybersecurity, information assurance, and data protection requirements.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The Security Architecture Definition (SAD) provides a comprehensive description of the NEXUS service cybersecurity architecture, including technical and operational security controls, encryption methods, security protocols, risk management approach, and continuous monitoring capabilities. The SAD addresses security across all system elements including space segment, ground segment, network infrastructure, user interfaces, and data management systems. The document demonstrates how the Contractor's security architecture protects NASA data, systems, and operations from cybersecurity threats and vulnerabilities while meeting applicable NASA security policies and Federal requirements. The SAD includes or references the Cybersecurity Assessment and Authorization (CASQ) package that documents the security authorization process, risk assessment results, security control implementation, and authorization decisions. The level of detail must be sufficient to enable Government assessment of cybersecurity posture, identification and mitigation of security risks, and informed authorization decisions.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:

NEXUS-RQMT-001	*Service Requirements Document (SRD)*
FIPS 140-3	*Security Requirements for Cryptographic Modules*
FISMA (as applicable)	*Federal Information Security Modernization Act*
NIST SP 800-53	*Security and Privacy Controls for Information Systems and Organizations*
CNSS	*Committee on National Security Systems*

15.3 **CONTENTS**: The Security Architecture Definition (SAD) must include the following:

a. Executive Summary:
   1. Overview of the security architecture approach.
   2. Security architecture philosophy and design principles.
   3. Summary of key security capabilities and controls.
   4. Compliance statement with NASA security requirements.
   5. Security authorization status.

b. System Security Context: The Contractor shall describe the system security context to establish an understanding of the operational environment, system scope, and security-relevant characteristics. This section is intended to inform the security architecture and does not prescribe or imply a specific facility or system security level.
   1. System description and operational environment.
   2. System boundaries and demarcation points.
   3. External Interfaces and Interconnections, including RF links, digital interfaces, and network connections.
   4. Dependencies on external services and infrastructure (e.g., communication networks, cloud providers, third-party ground stations).
   5. Information types and general data characteristics.
   6. Data flow diagrams showing information flows and security domains.
   7. Identification of assets requiring protection (data, systems, networks).
   8. Classification and sensitivity of data handled by the system.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

9. Identification of User types (e.g., administrators, operators, mission users) and general access patterns.
10 General description of anticipated threat environment (e.g., cyber threats to space-ground links, network intrusion, service disruption).

c. Security Architecture Design:
1. Overall security architecture framework and structure.
2. Security zones and domains.
3. Defense-in-depth strategy and layered security approach.
4. Security architecture diagrams and models.
5. Security design principles applied (e.g., least privilege, separation of duties).
6. Integration of security controls across system layers.
7. Secure-by-design features and capabilities.

d. Access Control and Authentication:
1. User authentication methods and multi-factor authentication.
2. Access control policies and role-based access control (RBAC).
3. Privileged user management and monitoring.
4. Account management and provisioning procedures.
5. Session management and timeout policies.
6. Remote access controls and VPN security.
7. Physical access controls for facilities and equipment.

e. Encryption and Cryptography:
1. Encryption methods for data at rest and data in transit.
2. Cryptographic algorithms and key lengths.
3. Key management architecture and procedures.
4. Certificate management and public key infrastructure (PKI).
5. Encryption for command and telemetry links.
6. Encryption for ground network communications.
7. Compliance with FIPS 140-3 for cryptographic modules – in addition, architecture should be engineered to enable future encryption standard revisions where possible. For example, AES with provision to implement ML-KEM.
8. End-to-end encryption capabilities.

f. Network Security:
1. Network architecture security design.
2. Firewall configurations and policies.
3. Intrusion detection and prevention systems (IDS/IPS).
4. Network segmentation and isolation.
5. Secure network protocols and standards.
6. Virtual private networks (VPN) and secure tunneling.
7. Wireless security measures, if applicable.
8. Denial of Service (DoS) protection mechanisms.
9. Network monitoring and traffic analysis capabilities.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

g. Security Controls Implementation:
   1. Detailed description of security controls implemented.
   2. Mapping of controls to NIST SP 800-53 or equivalent framework.
   3. Technical controls (e.g., firewalls, encryption, monitoring).
   4. Operational controls (e.g., procedures, training, incident response).
   5. Management controls (e.g., policies, risk management, oversight).
   6. Control implementation status and effectiveness.
   7. Compensating controls for any unimplemented or partially implemented controls.

h. Vulnerability Management and Patching:
   1. Vulnerability assessment and scanning procedures.
   2. Patch management process and schedules.
   3. Configuration management and secure baseline maintenance.
   4. Software and firmware update procedures.
   5. Security testing and evaluation approach.
   6. Penetration testing plans.

i. Security Monitoring and Incident Response - The Contractor must describe how security monitoring interfaces with broader service performance monitoring and anomaly detection systems to ensure coordinated identification and response to both cybersecurity and operational anomalies. Additionally, the Contractor's security monitoring and incident response plan must include:
   1. Continuous monitoring of architecture and capabilities.
   2. Security Information and Event Management (SIEM) implementation.
   3. Log collection, retention, and analysis.
   4. Anomaly detection and alerting mechanisms.
   5. Incident detection and response procedures.
   6. Incident reporting and coordination with NASA.
   7. Forensics capabilities and evidence preservation.
   8. Security metrics and performance indicators.

j. Data Protection and Privacy:
   1. Data protection measures throughout the data lifecycle.
   2. Data sanitization and disposal procedures.
   3. Backup and recovery security controls.
   4. Privacy protection measures for sensitive data.
   5. Data loss prevention (DLP) capabilities.
   6. Separation of customer data and multi-tenancy security.

k. Supply Chain Security:
   1. Supply chain risk management approach.
   2. Vendor and third-party security assessments.
   3. Hardware and software component security.
   4. Trusted sources for critical components.
   5. Software provenance and integrity verification.

DRD Continuation Sheet

TITLE: Security Architecture Definition (SAD) **DRD NO.**: **NEXUS-DRD-005**
DATA TYPE: 2 **PAGE**: 5/6

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

l. Security Governance and Management:
   1. Security organization and roles/responsibilities.
   2. Security policies, standards, and procedures.
   3. Security training and awareness programs.
   4. Security configuration management.
   5. Change control procedures for security-relevant changes.
   6. Compliance and audit processes.
   7. Security risk management framework

m. Cybersecurity Assessment and Authorization (CASQ) Package:
   1. System Security Plan (SSP) or equivalent documentation.
   2. Security assessment report and findings.
   3. Risk assessment methodology and results.
   4. Identified vulnerabilities and mitigation strategies.
   5. Plan of Action and Milestones (POA&M) for remediation items.
   6. Security authorization decision documentation.
   7. Authority to Operate (ATO) status and conditions.
   8. Continuous monitoring plan.

n. Security Requirements Traceability:
   1. Mapping of applicable, contractually levied NASA and NEXUS security requirements to implemented security controls, including identification of control implementation approach and any standards or frameworks used (e.g., NIST controls or equivalent).
   2. Compliance demonstration with NEXUS SRD security requirements (SP-1, SP-2, CS-11).
   3. Cross-reference to NEXUS-DRD-001, Service Requirements Compliance Matrix.
   4. Identification of any security requirement waivers or deviations.

o. Security Testing and Validation:
   1. Security testing approach and methodologies.
   2. Penetration testing results and remediation.
   3. Security control validation results.
   4. Cross-reference to Service Demonstration & Validation Plan
   5. Ongoing security assessment schedule.

p. Operational Security Considerations:
   1. Security constraints and operational limitations.
   2. Security considerations for contingency operations.
   3. Security incident handling during demonstration and operations.
   4. Security coordination procedures with NASA security teams.
   5. Security decommissioning and data disposition procedures.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

15.4 **FORMAT**: Contractor format is acceptable. The SAD may be submitted as a single consolidated document or as a document package with the CASQ artifacts provided separately or as appendices. Due to the sensitive nature of security information, the SAD must clearly mark security-sensitive sections and follow appropriate handling procedures. Detailed technical security information (e.g., firewall rules, encryption keys, vulnerability details) may be provided in classified annexes or supplementary documents with appropriate access controls. Electronic submission with appropriate encryption and access controls is required.

15.5 **MAINTENANCE**: The SAD must be maintained current throughout the Demonstration Phase and into operational service delivery. Changes and/or updates must be submitted in accordance with the schedule specified in Item 12, following any security architecture changes, after security assessments or audits, upon identification of new threats or vulnerabilities, or as requested by the Government. Significant security architecture changes must be coordinated with NASA security authorities prior to implementation. Routine operational changes, including the addition or removal of assets that conform to the defined architecture (e.g., spacecraft within a constellation), do not in themselves necessitate SAD updates. Security incidents, newly identified vulnerabilities, or changes to threat environment must be reported promptly per incident response procedures, with SAD updates submitted within 30 calendar days of incident resolution. The CASQ package must be updated annually or more frequently as required by NASA security policy. Changes and/or updating must be in accordance with the provider/contractor's approved change control system and security configuration management procedures. All updates must include revision history and summary of changes affecting security posture. Changes and/or updates must be in accordance with the provider/contractor's approved change control system.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: NEXUS **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-006**
3. **DATA TYPE**: 2
4. **DATE REVISED**:
5. **PAGE**: 1/7

6. **TITLE**: Service Transition Plan (STP)

7. **DESCRIPTION/USE**: This plan documents the strategy, activities, criteria, and timeline for transitioning the NEXUS service from the Demonstration Phase to Initial Operational Capability (IOC), and informs the structure and expectations for transition planning to be required under any subsequent Operational Service Contract, which will be competed separately and require all offerors to provide their own transition approach, enabling the Government to make informed transition decisions, assess IOC readiness, and ensure establishment of the technical and operational foundation for sustained service delivery.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief**: Not applicable; **CLIN 2 Authorization to Proceed + 30 days**: Initial Baseline; **Demonstration & Integration Maturity**: Final Baseline; **Demonstration Readiness Review**: Update as required; 6**Demonstration Performance Validation Review**: Update as required

12. **SUBMISSION FREQUENCY**: Update as required

13. **REMARKS**: This DRD supports the Government's need to enable a structured transition from Demonstration to Initial Operational Capability and prepares for follow-on Full Operational Capability (acquisition actions as identified in Attachment E of the Government Insight Deliverables document. The Service Transition Plan is a Type 2 data item subject to Government review and approval by exception, with a 45-calendar day review period. This plan is critical for enabling informed transition decisions and ensuring IOC readiness. The plan addresses transition readiness criteria tailored to the demonstration validation and transition readiness scope, recognizing that certain long-term operational artifacts may be deferred to a subsequent Full Operational Capability (FOC) contract.

14. **INTERRELATIONSHIP**: NEXUS-DRD-001, Service Requirements Compliance Matrix, NEXUS-DRD-002, Service Demonstration & Validation Plan, NEXUS-DRD-003, Verification Closure Notices, NEXUS-DRD-005, Security Architecture Definition, NEXUS-DRD-008, Service Financial & Pricing Structure Definition, NEXUS-DRD-010, Continuity of Service Operations Plan and applicable contract paragraphs [TBD] related to IOC criteria and transition requirements.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The Service Transition Plan (Demonstration through IOC) provides a comprehensive description of the Contractor's approach to transitioning the NEXUS service from Demonstration Phase to IOC. The plan defines sequence of activities required to achieve service delivery capability and establishes the timeline and milestones for transition execution. The plan addresses technical readiness, operational readiness, regulatory compliance readiness, infrastructure readiness, organizational readiness, and risk mitigation necessary to support sustained service delivery. The Service Transition Plan enables the Government to assess IOC readiness, make informed transition authorization decisions, and ensure that the technical and operational foundation for sustained service delivery has been established. The scope is tailored to support demonstration validation and transition readiness, recognizing that certain long-term operational artifacts (e.g., enforceable Service Level Agreements, full-service assurance frameworks, mature operational governance plans) may be deferred to a subsequent FOC contract.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:

NEXUS-RQMT-001 *NEXUS Service Requirements Document (SRD)*

15.3 **CONTENTS**: The Service Transition Plan must include the following:

a. Executive Summary:
   1. Overview of transition approach and philosophy.
   2. Transition timeline and major milestones.
   3. Summary of IOC readiness criteria.
   4. Key transition risks and mitigation strategies.
   5. Transition decision gates and approval authorities.

b. Transition Strategy and Approach:
   1. Transition objectives and success criteria.
   2. Phased transition approach (if applicable).
   3. Transition phases and major activities.
   4. Relationship between Demonstration Phase, IOC, and future FOC.
   5 Service activation strategy (e.g., limited initial service, phased user onboarding).
   6. Parallel operations approach (if demonstration and initial operations overlap).
   7. Fallback and contingency strategies.

c. IOC Readiness Criteria:
   1. Technical readiness criteria:
      (a) Verification closure status for NEXUS SRD requirements.
      (b) System performance validation against NEXUS SRD requirements.
      (c) Interface interoperability demonstration.
      (d) Service architecture validation at demarcation boundaries.
      (e) Hardware/software configuration readiness.
      (f) Spare equipment and redundancy availability.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

(g) Completion of end-to-end service validation demonstrating full-service chain performance.

(h) Validation of service performance under multi-user and representative operational loading conditions.

2. Operational readiness criteria:
   (a) Operational procedures documented and validated.
   (b) Mission operations center (MOC) or network operations center (NOC) readiness.
   (c) 24/7 operations capability (if required).
   (d) Customer support capabilities established.
   (e) Service ordering and provisioning systems operational, including customer interface mechanisms (e.g., API, portal, or equivalent) and supporting backend provisioning systems.
4. Infrastructure readiness criteria:
   (a) Space segment operational status.
   (b) Ground segment operational status.
   (c) Network infrastructure operational status.
   (d) Monitoring and control systems operational.
   (e) Backup and contingency systems operational.
5. Regulatory readiness criteria:
   (a) Export control compliance established.
   (b) Spectrum licenses and authorizations obtained.
   (c) Regulatory approvals in place for service delivery.
   (d) Cybersecurity authorization (ATO/ATC) obtained.
6. Business readiness criteria:
   (a) Service pricing structure defined and approved.
   (b) Customer agreements templates prepared.
   (c) Billing and financial management systems operational.
   (d) Insurance and liability coverage in place (if required).
7. Documentation readiness criteria:
   (a) User documentation and interface specifications available.
   (b) Operations manuals and procedures complete.
   (c) Training materials available.
   (d) Technical documentation baselines established.

d. IOC Readiness Assessment Process:
   1. Readiness assessment methodology and procedures.
   2. Readiness review schedule and milestones.
   3. Roles and responsibilities for readiness assessment.
   4. Government and Contractor participation in readiness reviews.
   5. Readiness Metrics and Key Performance Indicators (KPIs).
   6. Readiness evidence documentation and verification.
   7. Readiness status reporting format and frequency.
   8. Criteria for IOC authorization decision.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

e. Operational Activation Path:
   1. Detailed sequence of transition activities.
   2. Activity dependencies and critical path.
   3. Time-phased transition timeline with milestones.
   4. Transition from demonstration configuration to operational configuration.
   5. System commissioning and operational acceptance activities.
   6. Service activation procedures and checklists.
   7. Initial service delivery and user onboarding procedures.
   8. Operational handover from demonstration team to operations team.
   9. Configuration management transition.
   10. Documentation and data package turnover.

f. Technical Transition Activities:
   1. Final verification and validation completion.
   2. System configuration baseline establishment.
   3. Software version control and release management.
   4. Hardware acceptance and deployment.
   5. Interface verification and acceptance.
   6. Performance testing and acceptance demonstrations.
   7. Security certification and accreditation finalization.
   8. Anomaly resolution and closeout.
   9. Technical baseline documentation updates.

g. Operational Transition Activities:
   1. Operations team staffing and training completion.
   2. Operational procedures validation and approval.
   3. Operations facilities and infrastructure activation.
   4. Monitoring and control systems activation.
   5. Communications systems and networks activation.
   6. Customer support infrastructure establishment.
   7. Service desk and help desk activation.
   8. Operational rehearsals and simulations.
   9. Operational readiness exercises.
   10. Shift handover procedures implementation.

h. Operational Transition:
   1. Organizational structure for IOC operations.
   2. Roles and responsibilities definition.
   3. Staffing plan and resource allocation.
   4. Training and certification requirements.
   5. Personnel transition from demonstration to operations.
   6. Organizational interfaces and communication protocols.
   7. Escalation procedures and decision authorities.
   8. Contract transition considerations (if applicable).

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

i. Service Activation and User Onboarding:
   1. Service availability schedule and phasing.
   2. Initial customer identification and prioritization.
   3. User registration and account setup procedures.
   4. User training and orientation programs.
   5. Initial service provisioning procedures.
   6. User acceptance testing and verification.
   7. Feedback collection and issue resolution.
   8. Service expansion and scaling approach.

j. Risk Management and Mitigation:
   1. Transition risk identification and assessment.
   2. Technical risks to IOC achievement.
   3. Schedule risks and critical path dependencies.
   4. Regulatory risks and mitigation strategies.
   5. Operational risks and preparedness gaps.
   6. Resource and staffing risks.
   7. External dependencies and their status.
   8. Risk mitigation plans and contingency actions.
   9. Go/No-Go decision criteria and fallback plans.

k. Transition Support and Coordination:
   1. Government support requirements during transition.
   2. Coordination with NASA user community.
   3. Industry partner and subcontractor coordination.
   4. International partner coordination (if applicable).
   5. Regulatory agency coordination.
   6. Communication and stakeholder engagement plan.
   7. Transition status reporting and reviews.

l. Post-IOC Activities and Sustainment:
   1. Initial operational period objectives and monitoring.
   2. Service performance monitoring and reporting.
   3. Continuous improvement processes.
   4. Issue identification and resolution procedures.
   5. Service assurance and quality management.
   6. Operational metrics and KPI tracking.
   7. Lessons learned capture and incorporation.
   8. Path to Full Operational Capability (FOC).

m. Decommissioning and End-of-Service Considerations:
   1. High-level approach for end-of-service planning for all service segments (space, ground, and network).
   2. Space segment disposal strategy (e.g., deorbit, graveyard orbit, passivation, collision risk management) consistent with applicable orbital debris mitigation requirements (e.g., FCC Title 47 CFR 25.114, NASA-STD-8719.14).
   3. Service termination (e.g., customer notification timelines, continuity/transition plan).

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

4. Ground system decommissioning or transition strategy (e.g., shutdown, repurposing, or transfer), shutdown of user interfaces/APIs, cybersecurity closure (NIST alignment), data disposition and archival approach, including retention and transfer to the Government as applicable.
5. Service continuity considerations during phased decommissioning or provider transition.
6. Handover or transition approach to follow-on service providers or Government-managed systems (if applicable).
7. Identification of any long-lead regulatory, safety, or licensing considerations associated with decommissioning.

n. Transition Metrics and Status Tracking:

1. Readiness criteria tracking matrix.
2. Transition milestone status.
3. Key performance indicators for transition progress.
4. Issues and action items tracking.
5. Risk status dashboard.
6. Decision gate status and approval tracking.

o. Transition Documentation Package:

1. List of documentation required for IOC authorization.
2. Documentation delivery schedule.
3. Cross-references to other DRDs supporting IOC decision.
4. Technical data package contents.
5. Operational data package contents.
6. As-built documentation requirements.

p. Contractual and Business Considerations:

1. Contract transition from Demonstration to IOC/FOC.
2. Service agreement terms and conditions.
3. Performance incentives and penalties (if applicable).
4. Intellectual property and data rights considerations.
5. Warranty and guarantee provisions.
6. Service Level Agreement (SLA) framework (preliminary).

15.4 **FORMAT**: Contractor format is acceptable. The Service Transition Plan may be organized in sections, chapters, or phases as appropriate to the Contractor's transition approach. The IOC Readiness Criteria may be provided as an integrated section within the plan or as a separate controlled appendix. The plan may utilize charts, tables, Gantt charts, or other visual aids to illustrate the transition timeline, dependencies, and readiness status. Electronic format with searchable content and hyperlinks to support documentation is preferred.

DRD Continuation Sheet

TITLE: Service Transition Plan (STP) **DRD NO.**: **NEXUS-DRD-006**
DATA TYPE: 2 **PAGE**: 7/7

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

15.5 **MAINTENANCE**: The Service Transition Plan must be maintained current throughout the Demonstration Phase and updated through IOC achievement. Changes and/or updates must be submitted in accordance with the schedule specified in Item 12 or as requested by the Government. Quarterly updates are required during active transition periods, or more frequently as major transition milestones are achieved or transition risks change. Updates must reflect progress on transition activities, changes in readiness status, resolution of issues, changes to transition schedule or approach, and updated risk assessments. Significant delays in achieving transition milestones or identification of critical risks to IOC must be reported promptly to NASA, with updated plan submissions within 15 calendar days. A comprehensive final update must be submitted at least 60 calendar days prior to planned IOC authorization to support Government decision-making. Changes and/or updating must be in accordance with the provider/contractor's approved change control system. All updates must include revision history, summary of changes, and current readiness assessment against IOC criteria.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: NEXUS **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-007**
3. **DATA TYPE**: 2
4. **DATE REVISED**:
5. **PAGE**: 1/5

6. **TITLE**: Intellectual Property & Data Rights Management Plan (IPDRMP)

7. **DESCRIPTION/USE**: To document the Contractor's approach to managing intellectual property (IP) and data rights associated with the NEXUS service, including identification, marking, and protection of proprietary information, commercial data, and technical data submitted under the contract. This plan clarifies data rights assertions, establishes procedures for marking and handling proprietary data, and provides the Government with essential insight into IP considerations affecting demonstration execution and transition to operational service. The plan includes minimal provisions as specified in the contract to balance protection of Contractor intellectual property with Government need for appropriate rights and access to essential data.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination; limited distribution based on proprietary information sensitivity

11. **SUBMISSIONS**: **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief**: Not applicable; **CLIN 2 Authorization to Proceed + 30 days**: Initial Baseline; **Demonstration & Integration Maturity**: Final Baseline; **Demonstration Readiness Review**: Update as required; **Demonstration Performance Validation Review**: Update as required

12. **SUBMISSION FREQUENCY**: Update as required or when IP/data rights assertions change

13. **REMARKS**: Reference applicable Federal Acquisition Regulation (FAR) and NASA FAR Supplement (NFS) clauses governing data rights, technical data rights, and computer software rights. This DRD supports the Government's need to protect Government interests during demonstration execution. The Intellectual Property & Data Rights Management Plan is a Type 2 data item subject to Government review and approval by exception, with a 45-calendar day review period. Per the Government Insight Deliverables document, this DRD includes minimal provisions in the contract, consistent with a service-based acquisition philosophy that preserves Contractor flexibility in design and implementation approach while ensuring Government access to essential data for oversight and transition decisions.

14. **INTERRELATIONSHIP**: NEXUS-DRD-005, *Security Architecture Definition* and applicable contract paragraphs [TBD] related to data deliverables, data rights, and intellectual property.

DRD Continuation Sheet

TITLE: Intellectual Property & Data Rights Management Plan (IPDRMP) **DRD NO.**: **NEXUS-DRD-007**

DATA TYPE: 2 **PAGE**: 2/5

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The Intellectual Property & Data Rights Management Plan (IPDRMP) provides a streamlined description of the Contractor's approach to identifying, asserting, marking, and managing intellectual property rights and data rights for technical data, computer software, and other deliverables submitted under the NEXUS contract. Consistent with the service-based acquisition philosophy, the plan emphasizes minimal provisions necessary to protect Government interests while preserving Contractor flexibility and protecting commercial intellectual property. The plan clarifies which data will be delivered with unlimited rights, government purpose rights, limited rights, or restricted rights; establishes procedures for proper marking of proprietary and restricted data; and describes how the Contractor will manage data rights throughout the demonstration and operational phases. The level of detail is tailored to support Government oversight needs without imposing traditional development-focused data rights requirements that may not be appropriate for commercially provided services.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:

48 CFR Part 27	*Patients, Data, and Copyrights*
NFS 1827	*Patients, Data, and Copyrights*
FAR 52.227-14 (as applicable)	*Rights in Data – General*
FAR 52.227-23 (as applicable)	*Rights to Proposal Data (Technical)*
NEXUS-RQMT-001	*NEXUS Service Requirements Document (SRD)*

15.3 **CONTENTS**: The Intellectual Property & Data Rights Management Plan (IPDRMP) must include the following minimal provisions:

a. Executive Summary:
   1. Overview of IP and data rights management approach.
   2. Summary of data rights philosophy for service-based acquisition.
   3. Key IP considerations for NEXUS service.
   4. Balance between Contractor IP protection and Government access needs

b. Data Rights Categories and Assertions: The Contractor must ensure that data rights assertions enable Government access to a minimum set of technical data sufficient to support verification, interoperability, operational oversight, and potential transition to follow-on service providers. This set of data constitutes a minimum viable Technical Data Package (TDP), even in the context of a service-based acquisition.
   1. Description of data rights categories applicable to NEXUS contract:
      (a) Unlimited rights data.
      (b) Limited rights data (technical data).
      (c) Restricted rights data (computer software).
      (d) Proprietary commercial data.
      (e) Publicly available data.
   2. Data rights assertions by deliverable type:
      (a) Identification of which NEXUS DRDs will contain proprietary or restricted data.
      (b) Specific data rights asserted for each deliverable category.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

(c) Rationale for limited or restricted rights assertions.
(d) Identification of any specially negotiated data rights.

3. Technical data with asserted rights:
   (a) Hardware designs and specifications.
   (b) Software source code and documentation.
   (c) Processes and procedures.
   (d) Test data and analysis results.
   (e) Interface specifications.

c. Proprietary Data Identification and Marking:
   1. Procedures for identifying proprietary and restricted data.
   2. Marking requirements and procedures:
      (a) Proper legends for limited rights and restricted rights data.
      (b) Page-level and document-level marking practices.
      (c) Marking of proprietary commercial information.
      (d) Coordination of markings with export control markings.
   3. Examples of proper data rights markings.
   4. Procedures to ensure accurate and appropriate marking.
   5. Process for challenging or validating markings.
   6. Duration of restrictions and expiration procedures.

d. Data Handing and Protection Procedures:
   1. Government handling of proprietary and restricted data.
   2. Access control for limited-rights data.
   3. Non-disclosure agreements (if required).
   4. Storage and protection requirements.
   5. Distribution limitations.
   6. Procedures for Government personnel access to restricted data.
   7. Third-party access considerations (e.g., Government contractors).

e. Intellectual Property Consideration:
   1. Existing intellectual property (background IP):
      (a) Identification of pre-existing patents, copyrights, trademarks.
      (b) Background technology incorporated into NEXUS service.
      (c) Restrictions on Government use of background IP.
   2. Foreground intellectual property (developed under contract):
      (a) Ownership of IP developed during demonstration.
      (b) Rights to inventions and patents.
      (c) Copyright ownership for created works.
      (d) Treatment of improvements and modifications.
   3. Third-party intellectual property:
      (a) Licensed software and commercial off-the-shelf (COTS) products.
      (b) Subcontractor IP and data rights flow-down.
      (c) Open-source software usage and licensing.
      (d) Third-party license restrictions affecting Government use.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

4. Artificial Intelligence/Machine Learning (AI/ML) Data and Artifacts:
   (a) Identification of any AI/ML tools, models, or automated methods used in the development of contract deliverables.
   (b) Description of datasets used to train, fine-tune, or inform AI/ML models that contribute to deliverables.
   (c) Ownership and licensing of AI/ML models and associated training data.
   (d) Identification of any third-party, proprietary, or restricted datasets incorporated into AI-enabled outputs
   (e) Data rights implications for deliverables generated or assisted by AI/ML tools.
   (f) Any restrictions on Government use, modification, reproduction, or distribution of deliverables resulting from AI/ML usage.

f. Interface and Interoperability Data:
   1. Data rights approach for interface specifications (ICDs).
   2. Sufficient rights for Government interoperability needs.
   3. Balance between proprietary design protection and interface openness.
   4. Government's ability to procure compatible systems or services.
   5. API documentation and associated data rights.

g. Minimum Government Data Rights for Oversight:
   1. Essential data required for Government oversight with appropriate rights.
   2. Verification and validation data rights.
   3. Safety and mission assurance data rights.
   4. Data needed for IOC and FOC transition decisions.
   5. Rights sufficient to support Government acquisition objectives.
   6. Data required to support service performance monitoring, anomaly investigation, and operational assessment during demonstration and transition.

h. Commercial Data Protection:
   1. Protection of commercial pricing and cost data.
   2. Protection of commercial business practices and operations data.
   3. Treatment of commercially sensitive information.
   4. Restrictions on Government disclosure of commercial data.
   5. Freedom of Information Act (FOIA) considerations and exemptions.

i. Data Delivery and Access Procedures:
   1. Methods for delivering data with appropriate rights.
   2. Electronic data delivery and access controls.
   3. Data repositories and secure portals.
   4. Procedures for Government review of proprietary data.
   5. Controlled access provisions for sensitive technical data.
   6. Data retention and archiving requirements.

j. Software Data Rights:
   1. Rights in computer software and source code.
   2. Software documentation rights.
   3. Government's ability to use, modify, and reproduce software.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:
    4. Rights to software updates and maintenance releases.
    5. Escrow arrangements for critical software (if applicable).

k. Disputes and Resolution:
    1. Process for resolving data rights disputes.
    2. Challenge procedures for data rights assertions.
    3. Negotiation and clarification mechanisms.
    4. Escalation procedures.
    5. Contract modification procedures for data rights issues.

l. Data Rights for Follow-On Acquisitions:
    1. Data rights considerations for IOC and FOC contracts.
    2. Rights needed for competition (if applicable).
    3. Rights for follow-on service providers.
    4. Technical data package rights for sustainment.
    5. Considerations for multi-provided environment.

m. Compliance and Auditing:
    1. Contractor procedures to ensure proper data rights assertion.
    2. Internal review and validation of markings.
    3. Compliance with contract data rights clauses.
    4. Audit trail for data rights determinations.
    5. Correction procedures for improper assertions or markings.

n. Changes and Updates:
    1. Process for updating data rights assertions.
    2. Notification procedures for changes.
    3. Impact assessment for data rights changes.
    4. Government approval for significant changes.

15.4 **FORMAT**: Contractor format is acceptable. The IPDRMP should be concise and focused on minimal essential provisions, consistent with the service-based acquisition approach. The plan may include tables, matrices, or charts to clearly identify data rights by deliverable type. Data rights assertions may be provided in a separate controlled appendix or data rights assertion matrix. The format should facilitate easy Government review and understanding of what data will be available with what rights.

15.5 **MAINTENANCE**: The IPDRMP must be updated as required when there are changes to data rights assertions, when new deliverables are added to the contract, when intellectual property considerations change, or as requested by the Government. Because this DRD involves minimal provisions, updates are expected to be infrequent. Significant changes to data rights assertions that may affect Government oversight or transition capabilities must be submitted for review within 30 days of the proposed change. Changes and/or updating must be in accordance with the provider/contractor's approved change control system. All updates must include clear identification of changes from the previous version and rationale for any changes to data rights assertions.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-008**
3. **DATA TYPE**: 1
4. **DATE REVISED**:
5. **PAGE**: 1/6

6. **TITLE**: Service Financial & Pricing Structure Definition (SFPSD)

7. **DESCRIPTION/USE**: To document the Contractor's proposed commercial service pricing approach, assumptions affecting pricing, service tiers and options, pricing scalability, economic sustainability factors, transition from demonstration to operational service pricing, and major pricing risks and dependencies. The SFPSD provides the Government with sufficient insight to assess commercial viability, affordability, long-term service sustainability, and potential pricing-related risks to future service availability. The SFPSD is intended for use in evaluating whether the proposed service pricing approach is practical, scalable, and supportable over time within a commercial fixed-price service acquisition framework. This DRD does not require certified cost or pricing data, cost-accounting system information, Cost Accounting Standards (CAS) compliance information, indirect rate data, detailed cost build-ups, corporate financial statements, profit calculations, return-on-investment analysis, break-even analysis, EBITDA projections, or open-book accounting information.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination; limited distribution based on proprietary pricing and commercial sensitivity. The SFPSD may contain proprietary commercial pricing information and shall be marked and protected in accordance with applicable contract provisions.

11. **SUBMISSIONS**: **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief**: Not applicable; **CLIN 2 Authorization to Proceed + 30 days**: Initial Baseline; **Demonstration & Integration Maturity**: Final Baseline; **Demonstration Readiness Review**: Not applicable; **Demonstration Performance Validation Review**: Not applicable

12. **SUBMISSION FREQUENCY**: The SFPSD shall be updated when material pricing assumptions change, service tiers or pricing structures materially change, significant sustainability assumptions change, demonstration-to-operational transition pricing changes, or as requested by the Contracting Officer.

DRD Continuation Sheet

TITLE: Service Financial & Pricing Structure Definition (SFPSD) **DRD NO.**: **NEXUS-DRD-008**

DATA TYPE: 1 **PAGE**: 2/6

15. **DATA PREPARATION INFORMATION**:

13. **REMARKS**: The SFPSD is a Type 1 data item requiring formal Government review and approval. Government approval establishes the baseline pricing and sustainability approach for NEXUS service planning purposes; however, approval of this DRD does not constitute Government approval of the Contractor's internal business model, proprietary cost structure, or corporate financial strategy. The SFPSD supports Government assessment of commercial service viability, affordability, pricing stability, transition readiness, and long-term service sustainability. The Government's review is focused on whether the proposed pricing approach and supporting assumptions are reasonable, understandable, scalable, and adequately supported for commercial service delivery. This DRD is not intended to convert a fixed-price commercial services acquisition into a cost-type reporting construct.

14. **INTERRELATIONSHIP**: NEXUS-DRD-006, Service Transition Plan, NEXUS-DRD-007, Intellectual Property & Data Rights Management Plan, NEXUS-DRD-010, Continuity of Service Operations Plan (COSP) and applicable NEXUS contract Performance Work Statement (PWS) paragraphs related to pricing, service fees, payment terms, and contract financial management.

15.1 **SCOPE**: The Service Financial & Pricing Structure Definition (SFPSD) provides a comprehensive description of the financial framework, business model, price structure, and pricing approach for sustaining the NEXUS service throughout its operational life. The definition addresses the economic viability of the service, pricing methodologies, cost drivers, revenue projections, and financial sustainability plans for follow on service phases. The document provides the Government with essential insight into the financial aspects of service delivery necessary to support informed acquisition decisions, budget planning, and assessment of long-term service sustainability. The level of detail shall be sufficient to enable Government evaluation of pricing reasonableness, price realism, financial risk, and value proposition while respecting the commercially sensitive nature of detailed cost and pricing data.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:

FAR Part 15	*Contracting by Negotiation*
FAR Part 31	*Contract Cost Principles and Procedures*
NEXUS-RQMT-001	*NEXUS Service Requirements Document (SRD)*

15.3 **CONTENTS**: The Service Financial & Pricing Structure Definition (SFPSD) shall include the following:

a. Executive Summary:
   1. Overview of the proposed pricing approach.
   2. Summary of available service tiers or options.
   3. Summary of key assumptions affecting pricing.
   4. Overview of pricing scalability with user demand.
   5. Summary of long-term sustainability considerations.
   6. Summary of major pricing risks and dependencies.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

b. Proposed Service Pricing Approach: The contractor will describe the proposed service pricing approach. The description should address, as applicable.
   1. Fixed-price, subscription-based, usage-based, tiered, or hybrid pricing approach.
   2. Pricing structure for proposed services.
   3. Relationships between pricing and service capability.
   4. Basis for pricing, such as market-based, value-based, catalog-based, or commercial service pricing.
   5. Pricing validity period or conditions under which pricing may be updated.
   6. Approach for maintaining pricing stability over time.

   The Contractor is not required to provide cost build-ups, indirect rates, profit calculations, or cost-accounting information.

c. Assumptions Affecting Pricing: The Contractor will identify key assumptions that materially affect pricing. Assumptions should include, as applicable:
   1. Expected service utilization.
   2. Anticipated User demand.
   3. Capacity availability assumptions.
   4. Ground infrastructure assumptions.
   5. Spectrum and regulatory assumptions.
   6. Third-party service or infrastructure dependencies.
   7. Shared infrastructure assumptions.
   8. Technology refresh or modernization assumptions.
   9. Operational support assumptions.
   10. Government-furnished information, interface, facility, or support assumptions.

   The Contractor must identify assumptions that, if changed, could materially affect future pricing, affordability, or service availability.

d. Service Tiers and Options: The Contractor shall describe available service tiers, options, or ordering constructs. The description shall address, as applicable:
   1. Baseline service offering.
   2. Enhanced or premium service options.
   3. Priority service options.
   4. Optional capabilities.
   5. Service performance levels.
   6. User support options.
   7. Scalability or capacity options.
   8. Any distinctions between demonstration service offerings and operational service offerings.

   The Contractor shall explain how service tier, performance level, availability, support level, or optional capability may affect pricing.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

e. Pricing Scalability with User Demand: The Contractor shall describe how pricing may scale as user demand changes. The description shall address, as applicable:
   1. Increased utilization scenarios.
   2. Additional user or mission adoption.
   3. Capacity growth considerations.
   4. Pricing implications of increased demand.
   5. Economies of scale, if applicable.
   6. Potential constraints on pricing scalability.
   7. Conditions under which demand growth could require pricing adjustment.

   The Contractor is not required to provide revenue forecasts or detailed financial models.

f. Economic Sustainability of the Service: The Contractor shall describe the approach for sustaining commercial service delivery over the anticipated operational life. The description shall address, as applicable:
   1. Long-term service support approach.
   2. Capacity management approach.
   3. Infrastructure sustainment considerations.
   4. Technology refresh and modernization considerations.
   5. Factors supporting continued commercial availability.
   6. Relationship between service demand and sustained service viability.
   7. Major business, technical, operational, or market factors that could affect continued service delivery.

   The Contractor is not required to provide corporate financial statements, detailed investment plans, return-on-investment calculations, break-even analysis, EBITDA projections, or proprietary capital planning data.

g. Demonstration-to-Operational Service Pricing Transition: The Contractor shall describe the expected transition from demonstration-phase pricing to operational service pricing. The description shall address, as applicable:
   1. Demonstration-phase pricing approach.
   2. Planned operational service pricing approach.
   3. Expected pricing changes between demonstration and operational phases.
   4. Rationale for anticipated pricing changes.
   5. Assumptions supporting operational pricing.
   6. Factors that could affect affordability during transition.
   7. Approach for maintaining pricing continuity or stability during transition.

h. Major Pricing Risks and Dependencies: The Contractor should identify major risks and dependencies that could affect pricing, affordability, service scalability, or long-term sustainability. Examples may include:
   1. Regulatory changes.
   2. Spectrum availability or coordination constraints.
   3. Supply-chain constraints.
   4. Launch, replenishment, or infrastructure dependencies.
   5. Ground infrastructure availability

DRD Continuation Sheet

TITLE: Service Financial & Pricing Structure Definition (SFPSD) **DRD NO.**: **NEXUS-DRD-008**

DATA TYPE: 1 **PAGE**: 5/6

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

6. Third-party service dependencies.
7. Market demand uncertainty.
8. Technology obsolescence.
9. Capacity limitations.
10. Significant changes to Government requirements or service utilization assumption.
11. For each major risk or dependency, the Contractor will provide:
    (a) Description of the risk or dependency.
    (b) Potential pricing or sustainability impact.
    (c) Planned mitigation or management approach

i. Financial Risks and Mitigation:
1. Financial risk assessment
2. Risk mitigation strategies.
3. Financial contingency planning.
4. Insurance and financial guarantees.
5. Financial reserves and capitalization.

j. Sustainability and Long-Term Viability:
1. Service sustainability plan.
2. Financial requirements for sustained operations.
3. Technology refresh and modernization funding.
4. Spare capacity and redundancy funding.
5. Continuity of operations financial planning.
6. Cross-reference to Continuity of Service Operations Plan.
7. End-of-life and decommissioning costs.

k. Special Considerations and Assumptions:
1. Key assumptions underlying pricing structure.
2. Dependencies on customer volume or utilization.
3. Shared infrastructure or cost-sharing arrangements.
4. Government-furnished equipment or support impacts on pricing.
5. Research and development cost recovery approach.

l. IOC and FOC Pricing Transition:
1. Demonstration phase cost recovery approach.
2. IOC pricing structure and timeline.
3. FOC pricing structure and evolution.
4. Pricing changes from IOC to FOC and rationale.
5. Transition pricing for existing customers.
6. Price protection provisions.

m. Terms, Conditions, and Caveats:
1. Pricing validity period.
2. Conditions for pricing changes or renegotiation.
3. Regulatory change impacts on pricing.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:
    4. Most favored customer provisions (if applicable).
    5. Price matching or price guarantee terms.

15.4 **FORMAT**: Contractor format is acceptable. The SFPSD should emphasize concise narrative discussion supported by summary tables where useful. Pricing schedules, service tier summaries, assumption tables, and risk/dependency tables may be used to improve clarity. The following are not required and shall not be requested under this DRD unless separately required by contract clause:

1. Certified cost or pricing data.
2. CAS compliance information.
3. Cost-accounting system descriptions.
4. Detailed cost build-ups.
5. Cost allocation methodologies.
6. Indirect rate structures.
7. Profit calculations.
8. Open-book accounting information.
9. Audit procedures.
10. Corporate financial statements.
11. Revenue projections.
12. EBITDA analysis.
13. Break-even analysis.
14. Return-on-investment calculations.
15. Detailed CAPEX or OPEX reporting.

15.5 **MAINTENANCE**: The SFPSD shall be maintained current and updated as required when pricing structures change, when significant cost drivers change, when market conditions materially change, prior to contract negotiations for IOC or FOC phases, annually for cost and pricing updates, or as requested by the Government. Significant pricing changes shall be submitted for Government review and approval at least 90 calendar days prior to proposed implementation to allow for budget planning and contract modification processing. Updates shall include clear identification of changes from the previous version, rationale for pricing changes, and impact analysis on Government costs. Changes and/or updating shall be in accordance with the provider/contractor's approved change control system. All updates shall be marked as proprietary commercial information as appropriate and shall include revision history documenting the evolution of pricing structures over the contract lifecycle.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-009**
3. **DATA TYPE**: 2
4. **DATE REVISED**:
5. **PAGE**: 1/5

6. **TITLE**: Training Emulator

7. **DESCRIPTION/USE**: To provide an interface emulator capable of exercising the NEXUS forward and return service interfaces. The emulator must reproduce the external interfaces at the customer vehicle and customer control center demarcation boundaries, while representing the internal relay ("bent-pipe") behavior only at a generic or requirement-level abstraction sufficient to support interface interactions between those boundaries.

   The emulator enables customers, NASA, and the Government to test and validate interface interoperability, develop and test customer integration software, conduct operator training, and support integration and demonstration activities without requiring access to the operational NEXUS system.

   The emulator supports validation of service interfaces and operational interactions at defined demarcation boundaries during the Demonstration Phase. Implementation using commercially available emulation or test tools is encouraged, provided the emulator accurately represents the defined external interfaces and service behaviors.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **INITIAL SUBMISSION**: **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief**: Not applicable; **CLIN 2 Authorization to Proceed + 30 days**: Initial emulator delivery with basic functionality; **Demonstration & Integration Maturity**: Full-featured emulator with documentation; **Demonstration Readiness Review**: Update as required or requested by the Government; **Demonstration Performance Validation Review**: Not applicable

12. **SUBMISSION FREQUENCY**: Updates (with emulator version releases or interface changes)

13. **REMARKS**: This DRD supports the Government's need to assess technical feasibility and interface interoperability and enable validation of service architecture and interfaces at defined demarcation boundaries as identified in Attachment C of the Government Insight Deliverables document. The Interface Simulation is a Type 2 data item subject to Government review and approval by exception, with a 45-calendar day review period. The simulation provides a cost-effective and risk-reduced method for customers to develop and test integration software, conduct operator training, perform RF coverage analysis and run mission scenarios, and validate interface designs prior to operational system testing. The simulation scope is intentionally limited to interface-level fidelity and does not require detailed modeling of internal NEXUS system processing.

14. **INTERRELATIONSHIP**: NEXUS-DRD-002, Service Demonstration & Validation Plan, NEXUS-DRD-004, External Interface Control Documents (ICDs), Service Demonstration & Validation Plan and applicable contract paragraphs [TBD] related to interface validation and customer integration testing.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The Training Emulator deliverable provides a software-based emulator that reproduces the external behavior of the NEXUS forward and return service interfaces, enabling customers and the Government to exercise those interfaces without requiring access to the operational system.

The emulator must replicate the functional behavior of the NEXUS interfaces at the space and ground segments demarcation boundaries, allowing users to interact with the service interfaces as they would with the operational system.

The emulator must provide representative timing, data flow, and protocol behavior at the defined interfaces, while utilizing generic or requirement-level abstraction of the internal relay ("bent-pipe") data flow and processing between the two demarcation boundaries.

The emulator enables customers to develop, test, and validate integration software; conduct operator and mission personnel training; perform interface compatibility testing; validate interface specifications; and support demonstration planning and rehearsals.

The emulator scope is intentionally focused on external service interface behavior and does not require detailed modeling of internal NEXUS subsystems, spacecraft processing, or proprietary system implementations. The level of fidelity must be sufficient to enable meaningful interface interaction and interoperability testing while maintaining simplicity and ease of use.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:
NEXUS-RQMT-001 *NEXUS Service Requirements Document (SRD)*

15.3 **CONTENTS**: The Training Emulator deliverable shall include the following:

a. Emulator Package:
   1. Executable emulator software or configured Commercial off the Shelf (COTS) environment.
   2. Installation and deployment files.
   3. Required runtime libraries or dependencies.
   4. Platform compatibility information.
   5. Version identification and release notes.
   6. Identification of COTS Software Dependencies: Include cost and procurement lead time information for customers to procure licenses. (Example: Satellite Took Kit (STK)).

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

b. Interface Emulation - emulation of the forward (space-to-space) service interface including:
   1. Interface protocols.
   2. Data formats.
   3. Service request handling.
   4. Timing and latency characteristics (representative).

c. Return Service Interface - emulation of the return (space-to-space) service interface, including:
   1. Data delivery behavior.
   2. Interface protocol representation.
   3. Service timing behavior.

d. Ground Delivery Interface - Emulation of the ground-side service interface, including:
   1. Mission data delivery interface.
   2. Service request and scheduling interactions.
   3. Network interface behavior (logical representation).
   4. User interface API per NEXUS-DRD-004.

   The emulator must reproduce the functional behavior of the service interface sufficient for integration testing and mission preparation.

e. Service Behavior Representation - The emulator must represent external service characteristics, including:
   1. Representative data throughput ranges.
   2. Timing and latency behavior.
   3. Service access availability.
   4. Interface protocol exchanges.

   The emulator is not required to model internal spacecraft processing or proprietary algorithms.

f. Scenario Configuration - The emulator must allow configuration of test scenarios including:
   1. Mission timelines.
   2. Service Priority User List.
   3. Service requests and data transfers.
   4. Nominal and off-nominal service interactions.
   5. Resource availability conditions.
   6. Multi-user access scenarios.
   7. High-load or resource-constrained conditions.
   8. Degraded or off-nominal service behavior scenarios.

   These scenarios enable users to test operational interactions with the NEXUS service interfaces.

g. Input and Stimulus Capability - The emulator must allow users to provide input stimuli including:
   1. Command sequences.
   2. Service requests.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:
    3. Data transfers.
    4. Interface protocol messages.

h. Monitoring and Output - The emulator must provide monitoring and logging capabilities including:
    1. Interface message logging.
    2. Event timestamps.
    3. Status and activity monitoring.
    4. Performance statistics.

    Outputs must support interface verification and integration testing.

i. Documentation:
    1. Emulator User Guide.
        (a) Installation instructions.
        (b) Configuration instructions.
        (c) Scenario setup procedures.
        (d) Emulator operation instructions.
    2. Emulator Description.
        (a) Overview of emulator architecture.
        (b) Description of interface representations.
        (c) Modeling assumptions and limitations.

j. Validation - Approach used to verify that the emulator correctly represents the NEXUS external service interfaces as defined in the applicable interface specifications.

k. Version Management:
    1. Version identification.
    2. Change log and release notes.
    3. Updates reflecting changes to interface definitions.

15.4 **FORMAT**: Contractor format is acceptable. The Interface Simulation must be delivered as an executable software package with installation instructions and comprehensive user documentation. The simulation may be delivered on physical media (USB drive, CD/DVD) or via secure electronic download. Documentation may be provided in PDF format, HTML format for web-based access, or integrated help within the simulation application. Source code (if provided) must be well-commented and organized with appropriate development documentation. The simulation should be designed for ease of installation and use without requiring extensive specialized knowledge. A web-based or cloud-hosted version of the simulation may be provided as an alternative or supplement to locally installed software.

DRD Continuation Sheet

TITLE: Training Emulator **DRD NO.**: **NEXUS-DRD-009**
DATA TYPE: 2 **PAGE**: 5/5

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

15.5 **MAINTENANCE**: The Training Emulator must be maintained current and updated when significant interface changes occur, when errors or limitations are discovered that impact usefulness for interface testing, when additional capabilities are needed to support demonstration or testing activities, or as requested by the Government. Updates must be provided in accordance with the schedule specified in Item 12. The simulation must be updated to remain consistent with the Interface Control Documents (ICDs) and Application Programming Interface (API) specifications as they evolve. Major simulation updates or version changes must be communicated to customers at least 30 calendar days in advance when possible. All updates must include version identification, release notes describing changes, and instructions for upgrading from previous versions. Changes and/or updating must be in accordance with the provider/contractor's approved change control system. The Contractor must maintain a defect tracking system for reported issues and provide periodic status on issue resolution.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-010**
3. **DATA TYPE**: 3
4. **DATE REVISED**:
5. **PAGE**: 1/7

6. **TITLE**: Continuity of Service Operations Plan (CSOP)

7. **DESCRIPTION/USE**: To ensure the Contractor demonstrates a credible, architecture-level approach to continuity of service, rather than a component-level or prescriptive implementation. The plan should demonstrate how the provider will recover after the loss of an asset (e.g., spacecraft, ground station, etc.), including the approach for closing gaps in service, expected timelines for service restoration, and how these considerations are incorporated into the Contractor's overall service and cost strategy.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief**: Not applicable; **CLIN 2 Authorization to Proceed + 30 days**: Initial Baseline; **Demonstration & Integration Maturity**: Final Baseline; **Demonstration Readiness Review**: Update as required. **Demonstration Performance Validation Review**: Update as required

12. **SUBMISSION FREQUENCY**: Update or annually or following significant changes to service architecture or asset configuration

13. **REMARKS**: This DRD supports the Government's need to identify and mitigate risks to service continuity and IOC readiness and ensure establishment of the technical and operational foundation for sustained service delivery as identified in Attachment E of (Government Insight Deliverables) of the NEXUS Statement of Objectives. The Continuity of Service Operations Plan is a Type 3 data item subject to Government review and approval by exception, with a 45-calendar day review period. This plan is critical for assessing the resilience and reliability of the NEXUS service and for understanding the financial implications of service recovery and continuity provisions. The plan addresses both planned and unplanned interruptions or degradations to NEXUS service delivery that impact the Contractor's ability to meet defined service performance or availability commitments across all system elements. Industry standards for business continuity and disaster recovery planning.

14. **INTERRELATIONSHIP**: NEXUS-DRD-001, Service Requirements Compliance Matrix, NEXUS-DRD-006, Service Transition Plan, NEXUS-DRD-008, Service Financial & Pricing Structure Definition and applicable contract paragraphs [TBD] related to service availability, reliability, and continuity requirements.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The Continuity of Service Operations Plan (CSOP) provides a comprehensive description of the Contractor's approach to maintaining service continuity and recovering operations following the loss or degradation of critical assets including spacecraft, ground stations, network infrastructure, operations centers, or other system elements. The plan addresses both planned outages (e.g., maintenance, upgrades, replacements) and unplanned disruptions (e.g., failures, accidents, natural disasters, cyber incidents), defining redundancy strategies, backup capabilities, recovery procedures, service restoration timelines, and the financial provisions supporting continuity and recovery. CSOP demonstrates the resilience of the NEXUS service architecture and the Contractor's preparedness to maintain service availability and reliability throughout the operational life of the system. The plan enables the Government to assess risks to service continuity, evaluate the adequacy of redundancy and backup provisions, understand recovery timelines and service gaps, and verify that continuity provisions are financially sustainable and included in pricing structures.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:
NEXUS-RQMT-001 *NEXUS Service Requirements Document (SRD)*

15.3 **CONTENTS**: The Continuity of Service Operations Plan (CSOP) shall include the following:

a. Executive Summary:
   1. Overview of continuity of operations approach and philosophy.
   2. Summary of redundancy and backup capabilities.
   3. Key resilience features and service protection strategies.
   4. Service continuity objectives and commitments.
   5. Financial sustainability of continuity provisions.

b. Continuity of Operations Strategy:
   1. Overall approach to service continuity and resilience.
   2. Consideration of spectrum availability, interface, and coordination with external users as factors affecting service continuity.
   3. Design philosophy for fault tolerance and graceful degradation.
   4. Redundancy strategy across system elements.
   5. Backup and spare asset strategy.
   6. Single point of failure identification and mitigation.
   7. Planned vs. unplanned outage management.
   8. Service prioritization during degraded operations.

c. Asset Inventory and Criticality Assessment:
   1. Complete inventory of critical assets:
      (a) Space segment assets (e.g., satellites, spacecraft, payloads).
      (b) Ground segment assets (e.g., ground stations, antennas, terminals).
      (c) Network infrastructure (e.g., routers, switches, communication links).
      (d) Operations centers and control facilities.
      (e) Data centers and computing infrastructure.
      (f) Software systems and applications.
   2. Criticality assessment and impact analysis for each asset type.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:
    3. Single points of failure (if any) within the overall architecture (spacecraft and ground station).
    4. Dependencies and interdependencies between assets.
    5. Mean Time Between Failures (MTBF) and reliability data.
    6. Asset lifecycle and replacement schedules.

d. Spacecraft/Space Segment Continuity:
    1. Spacecraft constellation architecture and redundancy.
    2. Number of operational spacecraft and spares.
    3. On-orbit spare activation procedures and timelines.
    4. Launch and replenishment strategy for failed or degraded spacecraft.
    5. Spacecraft failure scenarios and impact analysis:
        (a) Single spacecraft loss.
        (b) Multiple spacecraft loss.
        (c) Partial payload/subsystem failure.
        (d) Orbital debris collision or damage.
    6. Service degradation analysis and workarounds.
    7. Recovery timeline after spacecraft loss.
    8. Service gap duration and minimization strategies.
    9. Interim service alternatives during spacecraft replacement.

e. Ground Segment Continuity - Ground station network architecture and geographic distribution:
    1. Ground station redundancy and backup capabilities.
    2. Mobile or transportable ground station options.
    3. Ground station failure scenarios and impact:
        (a) Single ground station loss.
        (b) Regional ground station outages.
        (c) Equipment failures.
        (d) Natural disasters affecting ground facilities.
    4. Alternate ground station activation procedures.
    5. Recovery timelines and service restoration.
    6. Equipment spare parts and maintenance provisions.

f. Network and Communications Infrastructure Continuity:
    1. Network architecture redundancy, including identification of potential common-cause failure risks and corresponding mitigation strategies.
    2. Internet service provider (ISP) redundancy.
    3. Network operations center (NOC) backup and alternate sites.
    4. Communications link failures and restoration.
    5. Cybersecurity incident response and recovery.
    6. Distributed denial of service (DDoS) mitigation.
    7. Network equipment spares and replacement.

g. Data Center and Computing Infrastructure Continuity:
    1. Data center redundancy and geographic diversity.
    2. Backup data center capabilities.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:
    3. Failover and disaster recovery procedures.
    4. Data backup and replication strategies.
    5. Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
    6. Cloud computing redundancy and availability.
    7. Database backup and restoration procedures.

h. Operations Center Continuity:
    1. Primary operation(s) center location and capabilities.
    2. Backup/alternate operations center facilities.
    3. Remote operations capabilities.
    4. Operation(s) center failover timelines.

i. Service Recovery Procedures:
    1. Decision-making authority and escalation procedures.
    2. Customer notification and communication during outages.

j. Service Recovery Timelines:
    1. Recovery Time Objectives (RTO) for each scenario:
        (a) Spacecraft loss recovery time.
        (b) Ground station loss recovery time.
        (c) Network infrastructure recovery time.
        (d) Data center failover time.
        (e) Operations center failover time.
    2. Service gap duration analysis and mitigation.
    3. Factors affecting recovery timelines.
    4. Best case, expected, and worst-case recovery scenarios.
    5. Comparison to service level requirements and commitments.

k. Interim Service and Workarounds:
    1. Temporary service alternatives during asset recovery:
        (a) Reduced service capacity or coverage.
        (b) Degraded service quality or data rates.
        (c) Alternative communication paths or routing.
        (d) Commercial service augmentation.
    2. Customer impact during interim service periods.
    3. Communication strategy with affected customers.

l. Spare Assets and Inventory Management:
    1. Spare spacecraft inventory and positioning:
        (a) Ground spares ready for launch.
        (b) On-orbit spares and positioning strategy.
        (c) Spare procurement and replacement schedule.
    2. Ground equipment spares:
        (a) Antenna and RF equipment spares.
        (b) Network equipment inventory.
        (c) Computing and storage equipment spares.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

The scope should be described at a functional level, addressing redundancy strategies, availability of critical ground infrastructure (e.g., gateways, antennas, network nodes), and replacement/supply chain approaches sufficient to sustain required service performance.

3. Spare parts logistics and supply chain.
4. Inventory management and replenishment triggers.
5. Vendor agreements for rapid equipment replacement.

m. Redundancy and Backup Testing:
1. Redundancy testing and validation procedures.
2. Failover testing schedule and frequency.
3. Backup system activation exercises.
4. Recovery procedure validation and rehearsals.
5. Lessons learned and continuous improvement.
6. Test results and performance verification.

n. Risk Assessment and Mitigation:
1. Service continuity risk identification:
(a) Likelihood and consequence of asset losses.
(b) Single points of failure.
(c) Common mode failures.
(d) Correlated risks (e.g., regional disasters).
2. Risk mitigation strategies and controls.
3. Residual risks and accepted vulnerabilities.
4. Risk monitoring and early warning systems.
5. Risk-based decision making for recovery investments.
6. Risks associated with radio frequency interference, spectrum congestion, and co-located system interactions.

o. Insurance and Liability Coverage:
1. Space-asset insurance coverage:
(a) Launch insurance.
(b) In-orbit insurance.
(c) Third-party liability insurance.
2. Ground asset and property insurance.
3. Business interruption insurance.
4. Cyber insurance coverage.
5. Insurance claim procedures and timelines.
6. Self-insurance or risk retention strategies

p. Supply Chain and Vendor Continuity:
1. Critical vendor and supplier identification.
2. Vendor business continuity requirements and assessment.
3. Alternate suppliers and sole-source risk mitigation.
4. Supply chain disruption scenarios and impacts.
5. Vendor agreements for emergency support and rapid response.
6. Parts obsolescence and technology refresh planning.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

q. Organizational and Personnel Continuity:
   1. Key personnel identification and succession planning.
   2. Cross training and knowledge management.
   3. Personnel backup and depth on critical functions.
   4. Contractor business continuity and financial stability.
   5. Subcontractor continuity provisions.
   6. Workforce health and safety during emergencies.

r. Communication and Coordination:
   1. Customer notification procedures during outages.
   2. Government coordination and reporting during incidents.
   3. Status updates and situational awareness reporting.
   4. Media and public relations during major incidents.
   5. Incident command structure and emergency management.
   6. Coordination with regulatory authorities (e.g., NTIA, FCC, FAA, ITU).

s. Continuous Improvement and Plan Maintenance:
   1. Lessons learned from actual incidents and exercises.
   2. Plan review and update procedures.
   3. Continuous improvement of recovery capabilities.
   4. Technology upgrades and modernization.
   5. Monitoring of service continuity performance metrics.
   6. Post-incident review and corrective actions.

t. Regulatory and Contractual Considerations: This section requires the Contractor to describe its standard regulatory and contractual practices for maintaining service continuity across its commercial customer base. The intent is to provide the Government with insight into how the Contractor defines, manages, and enforces continuity of service in its existing or planned commercial operations. Specifically, the Contractor shall describe:
   1. How Service Level Agreements (SLAs) are structured and enforced for commercial customers.
   2. Typical availability and reliability commitments, including how they are measured and tracked.
   3. Force majeure provisions, including key exclusions and how service continuity is addressed during such events.
   4. Use of service credits or penalties for outages or service degradation (as implemented in commercial agreements).
   5. Customer obligations during service disruptions, including any required actions or dependencies.
   6. Notification practices, including how and when customers (and, where applicable, the Government) are informed of disruptions or degraded service.

   This information is provided for Government insight into the Contractor's commercial service model, operational maturity, and approach to continuity of service. It is not intended to define, duplicate, or override NASA-specific contractual terms, remedies, or notification requirements, which will be established separately in the contract.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:
    u. Demonstration and IOC Considerations:
        1. Continuity provisions during Demonstration Phase.
        2. Transition from demonstration to operational redundancy.
        3. IOC readiness criteria related to continuity.
        4. Evolution of continuity capabilities toward FOC.
        5. Relationship to long-term operational artifacts deferred to FOC.

15.4 **FORMAT**: Contractor format is acceptable. CSOP should be organized logically by asset type, scenario, or functional area. Recovery procedures may be provided as appendices with detailed checklists and workflows. Financial information may be provided in tables or spreadsheets showing cost breakdowns and funding sources. Financial information may be provided in tables or spreadsheets to present targeted cost breakdowns and associated funding sources directly supporting continuity of service provisions. This information is intended to substantiate the feasibility of the Contractor's continuity approach and is not a comprehensive financial disclosure, but rather focused financial insight relevant to this DRD, given that no separate Financials DRD exists. Timelines and schedules may be illustrated with Gantt charts or diagrams. The plan may include figures, diagrams, or system architecture drawings to illustrate redundancy and backup capabilities. Sensitive information regarding specific vulnerabilities or security details must be appropriately protected and may be provided in a controlled or limited distribution format in accordance with applicable cybersecurity, export control, and data protection requirements. Such information may be excluded from general distribution versions of this DRD and provided separately to the Government upon request.

15.5 **MAINTENANCE**: The CSOP shall be maintained current and updated as required when service architecture changes significantly, when new assets are deployed or existing assets are retired, when redundancy or backup capabilities change, following actual service disruptions or recovery events, after continuity exercises or tests, when financial provisions for continuity change, or as requested by the Government. Annual updates are required to reflect operational experience, lessons learned, and evolving capabilities. Significant changes affecting recovery timelines or service gaps shall be reported to the Government within 30 calendar days. Changes and/or updating shall be in accordance with the provider/contractor's approved change control system. All updates shall include revision history, summary of changes, and assessment of impacts on service continuity and recovery capabilities. Actual recovery events and their outcomes shall be documented and used to refine the plan and improve future response.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-011**
3. **DATA TYPE**: 2
4. **DATE REVISED**:
5. **PAGE**: 1/5

6. **TITLE**: Verification/Validation Compliance Report (VVCR)

7. **DESCRIPTION/USE**: Defines the Contractor's end-to-end approach for demonstrating both verification and validation compliance with all NEXUS Service Requirements (SRD) and provides a current assessment of compliance status at the time of submission.

   The VVCR serves as the primary Verification Compliance Approach milestone deliverable, enabling the Government to:
   1. Assess the completeness, credibility, and traceability of the Contractor's verification strategy.
   2. Evaluate alignment between requirements, verification methods, and planned evidence.
   3. Understand the current state of compliance maturity across all SRD requirements.
   4. Identify verification risks, gaps, and dependencies prior to demonstration execution.

   The VVCR builds directly upon the Service Requirements Compliance Matrix (SRCM) and establishes the foundation for requirement closure via Verification Compliance Notices (VCNs) as defined in NEXUS-DRD-003.

   This deliverable supports a service-based verification paradigm where compliance is demonstrated through a combination of:
   1. Demonstration and operational evidence.
   2. Analysis and modeling/simulation.
   3. Inspection of records (IoR).
   4. Test and validation activities.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: **Verification Compliance Approach Milestone:** Preliminary VVCR submission; CLIN1 Design Outbrief; Not applicable; **CLIN 2 Authorization to Proceed + 30 days**: Update; **Demonstration & Integration Maturity**: Update; **Demonstration Readiness Review**: Update; **Demonstration Performance Validation Review**: Final VVCR submission

12. **SUBMISSION FREQUENCY**: Update as required or at major lifecycle milestones where compliance status or approach changes

13. **REMARKS**: The VVCR provides a requirement-driven assessment of verification and validation approach and compliance status. The VVCR must remain fully traceable (NEXUS-DRD-001 and NEXUS SRD. This DRD supports a Program/Project Inspection-of-Records (IoR)-enabled verification strategy for NEXUS SRD requirements closure.

15. **INTERRELATATIONSHIP:** NEXUS-DRD-001, Service Requirements Compliance Matrix, NEXUS-DRD-002, Service Demonstration & Validation Plan, NUXUS-DRD-003, Verification Closure Notices and applicable contract paragraphs [TBD] related to verification and compliance demonstration.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The Verification/Validation Compliance Report (VVCR) is a requirement-driven assessment of verification approach, verification execution status, validation status, and overall compliance posture for NEXUS SRD requirements. It does not define detailed demonstration scenarios, test procedures, or execution timelines, which are the responsibility of NEXUS-DRD-002, Service Demonstration & Validation Plan. The VVCR also does not serve as a requirement closure artifact; formal verification closure is documented per NEXUS-DRD-003, Verification Compliance Notices. In addition to documenting verification and validation status achieved during demonstration activities, the VVCR must identify all requirements that remain open, partially verified, partially validated, or conditionally closed at the completion of demonstration flight activities. For such requirements, the Contractor must provide the planned post-demonstration verification and validation approach, including identification of remaining evidence, analyses, operational data, inspections, demonstrations, or other objective evidence required to achieve full requirement closure and support transition toward operational service readiness.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:

NEXUS-RQMT-001 *NEXUS Service Requirements Document (SRD)*

15.3 **CONTENTS**: The Verification/Validation Compliance Report (VVCR) shall include the following:

a. Overview of Verification Compliance Approach.
   1. Summary of overall verification and validation philosophy and strategy describing:
      (a) Verification of SRD requirements.
      (b) Validation of mission/service objectives and backwards compatibility.
   2. Description of how the Contractor ensures:
      (a) Complete requirement coverage (verification).
      (b) Operational relevance and mission effectiveness (validation).
   3. Integration of:
      (a) Demonstration activities.
      (b) Operational service data.
      (c) Analysis and simulation.
      (d) Inspection of Records (IoR).

b. Traceability and Coverage Requirements.
   1. Mapping all of NEXUS SRD requirements to:
      (a) Lower-level derived and/or decomposed requirements.
      (b) Verification methods.
      (c) Validation activities (where applicable).

15. **DATA PREPARATION INFORMATION (CONTINUED)**:
    - (e) Planned evidence.
    - (f) Responsible systems or service elements.
  - 2. Explicit linkage to the Service Requirements Compliance Matrix (SRCM).
  - 3. Identification of:
    - (a) Requirements requiring validation (e.g., performance in operational context, end-to-end service delivery).
    - (b) Requirements satisfied solely through verification.
    - (c) Fully covered requirements.
    - (d) Partially covered requirements.
    - (e) Requirements with no defined verification approach.
- c. Verification Methods and Rationale.
  - 1. For each requirement (or grouped requirements), provide:
    - (a) Selected verification method(s):
      - (1) Test.
      - (2) Analysis.
      - (3) Demonstration.
      - (4) Inspection (including IoR).
    - (b) Selected Validation approach.
    - (c) Associated mission scenarios or use cases.
    - (d) Operational context in which validation will occur.
    - (e) Rational for scenario selection.
  - 2. Rational for verification method selection, including:
    - (a) Suitability for service-based verification.
    - (b) Feasibility and credibility.
    - (c) Alignment with demonstration-based verification.
- d. Planned Verification and Validation Evidence.
  - 1. Verification Evidence:
    - (a) Description of objective evidence to be generated for each requirement, including:
      - (1) Test results and logs.
      - (2) Demonstration outputs.
      - (3) Telemetry and operational data.
      - (4) Analysis products and models.
      - (5) Compliance matrices and certifications.
  - 2. Identification of:
    - (a) Data sources.
    - (b) Data fidelity and resolution.
    - (c) Evidence format and accessibility.
  - 3. Validation Evidence.
    - (a) Demonstration results under mission-representative conditions.
    - (b) End-to-end service performance data.
    - (c) User-level service outcomes (e.g., data delivery, latency, availability).

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

e. Current Verification and Validation Compliance Status.
   1. Provide a requirement-by-requirement status assessment, such as:
      (a) Verified (objective evidence available).
      (b) Validated (demonstrated in mission-representative context).
      (c) Partially compliant (partial evidence or pending validation).
      (d) Planned (verification/validation approach defined, not yet executed).
      (e) Not compliant/gap identified.
   2. Include:
      (a) Supporting rationale for status.
      (b) Reference to available evidence (if applicable).
      (c) Planned path to achieve compliance.

f. Validation Scenarios and Mission Use Cases.
   1. Description of key validation scenarios, including.
      (a) End-to-end service delivery.
      (b) Representative mission timelines.
      (c) Operational constraints and environments.
   2. Mapping of Scenarios to:
      (a) SRD requirements.
      (b) Mission objectives.

g. Verification Maturity Assessment.
   1. Overall assessment of:
      (a) Verification completeness.
      (b) Validation readiness.
   2. Identification of:
      (a) High-risk requirements.
      (b) Immature verification areas.
      (c) Unvalidated mission scenarios.
      (d) Dependencies on demonstration or operational conditions.

h. Risks, Gaps, and Assumptions.
   1. Identification of verification/validation-related:
      (a) Risks (technical, schedule, integration).
      (b) Gaps in approach or coverage.
      (c) Key assumptions impacting compliance.
   2. Mitigation strategies and planned resolution paths,

i. Integration with Demonstration and Operations.
   1. Description of how verification and validation activities are achieved through:
      (a) Demonstration scenarios.
      (b) Operational service delivery.
   2. Identification of:
      (a) Verification and validation events embedded within demonstration.
      (b) Use of operational data for compliance.

15. **DATA PREPARATION INFORMATION CONTINUED)**:
    j. Transition to Verification Closure (VCNs).
        1. Description of how verification results will be:
            (a) Captured.
            (b) Evaluated.
            (c) Submitted as VCNs.
        2. Description of how validation results support or inform closure decisions (where applicable).
        3. Mapping between VVCR content and eventual VCN submittals.
    k. Configuration and Data Management:
        1. Description of how verification and validation data and evidence are:
            (a) Controlled.
            (b) Versioned.
            (c) Traceable to requirements.
        3. Identification of tools and systems supporting:
            (a) Traceability (e.g., SRCM linkage).
            (b) Data integrity and auditability.

15.4 **FORMAT**: Contractor format is acceptable. The report must be organized to enable clear traceability to SRD requirements and easy identification of compliance status and gaps. Recommended formats include tables aligned with the SRCM structure; dashboards or visual summaries of compliance status; appendices for detailed mappings or evidence descriptions. The VVCR may include figures, diagrams, and architecture views, integrated compliance matrices, links or references to supporting data repositories.

15.5 **MAINTENANCE**: The VVCR must be updated when verification approach changes, significant compliance progress is made, and/or new risks or gaps are identified. Updates must clearly identify changes from previous submissions and maintain consistency with the SCRM and SRD baseline. Changes and/or updates must be submitted in accordance with the schedule specified in Item 12 or as requested by the Government.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-012**
3. **DATA TYPE**: 1
4. **DATE REVISED**:
5. **PAGE**: 1/5

6. **TITLE**: CLIN 1 Design Outbrief Package

7. **DESCRIPTION/USE**: The intent of this DRD is to review the current status of the design and to confirm that the design is ready for system integration. The package documents the Contractor's proposed NEXUS service solution, maturity of the technical and programmatic approach, current requirements compliance posture, major risks, and readiness to proceed into the demonstration planning and execution phase.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: No later than 30-calendar days prior to the conclusion of CLIN 1 period of performance, or as specified in the contract. **Oral Presentation** must follow the delivery of the written package.

12. **SUBMISSION FREQUENCY**: One-time submittal. Updates may be requested by the Government to support clarification, decision-making, or continuation planning.

13. **REMARKS**: This DRD supports NASA's assessment of the Contractor's readiness to proceed into CLIN 2. The written report must be concise and decision focused. Appendices may contain supporting technical details, data, analyses, and substantiating material, but must not be used to avoid providing the required substantive discussion in the main body of the report. This DRD provides a point-in-time artifact and must not duplicate detailed content required by other DRDs. The Contractor may summarize or reference supporting DRDs, analyses, and data products where appropriate.

14. **INTERRELATIONSHIP**: NEXUS-DRD-001, Service Requirements Compliance Matrix, NEXUS-DRD-002, Service Demonstration & Validation Plan, NEXUS-DRD-003, Verification Closure Notices, NEXUS-DRD-006, Service Transition Plan (STP), NEXUS-DRD-004, External Interface Control Documents (ICDs), NEXUS-RD-013, CLIN 2 Demonstration Readiness Package and applicable contract paragraphs [TBD] related to verification and compliance demonstration.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The CLIN 1 Design Outbrief Package must provide the Government with sufficient information to determine whether the Contractor's proposed NEXUS service solution, technical approach, requirements compliance posture, execution plan, and risk posture are sufficiently mature and credible to proceed into CLIN 2.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:
The package must address the Contractor's proposed architecture, demonstration concept, verification and validation approach, technical maturity, external interface approach, security and regulatory approach, schedule, risk posture, transition-to-service concept, and intellectual property/data rights approach.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:
NEXUS-RQMT-001 *NEXUS Service Requirements Document*

15.3 **CONTENTS**: The CLIN 1 Design Outbrief Package must include, at a minimum, the following:

a. Executive Summary: A concise summary of the proposed service solution, key decision points, major risks, open issues, and Contractor's assessment of readiness to proceed into CLIN 2.
b. Proposed End-to-End System Architecture and Design Solution: Description of the proposed NEXUS service architecture, including space segment, ground segment, network/service delivery architecture, service demarcation boundaries, major design features, and architectural trades or assumptions.
c. Concept of Operations Summary: Updated summary of the proposed operational concept for the NEXUS service architecture, including representative end-to-end operational scenarios demonstrating how users will request, receive, utilize, monitor, and manage services across the defined demarcation boundaries. The summary must describe operational roles and responsibilities, service execution flows, nominal and contingency operational concepts, and interactions between space, ground, network management, scheduling, cybersecurity, and user interface elements. The discussion should emphasize operational feasibility, scalability, and alignment with the proposed transition-to-service approach.
d. Requirements Compliance Posture: Summary of current compliance with NEXUS SRD requirements, including compliant areas, partial compliance, planned compliance, non-compliances, waivers/deviations, and major compliance risks. Detailed compliance data may be provided by reference per NEXUS-DRD-001, Service Requirements Compliance Matrix (SRCM).
e. Verification and Validation Approach: Summary of the planned approach for verifying and validating NEXUS SRD requirements during CLIN 2, including planned methods, key validation scenarios, demonstration objectives, and use of analysis, test, demonstration, inspection, or Inspection of Records, as applicable.
f. Technical Maturity Assessment: Updated assessment of hardware, software, networking, cybersecurity, automation, and operational technologies supporting the proposed NEXUS architecture. The assessment must identify critical technologies, current maturity status, remaining maturation activities, associated technical risks, and planned mitigation strategies. The discussion should identify any technologies requiring significant additional development, integration, qualification, or operational validation prior to service implementation and must include an assessment of impacts to schedule, cost, performance, or operational readiness.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

g. Technical, Schedule, and Cost Risk Assessment: Identification of major technical, schedule, cost, regulatory, security, interface, and operational risks, including mitigation plans, current mitigation status, residual risk, and risk impacts to CLIN 2 execution.

h. Launch Services and Regulator Compliance Approach: Summary of the planned launch services approach and the status of applicable regulatory, licensing, spectrum management, export control, and compliance activities associated with the proposed demonstration and operational architecture. The summary must identify major regulatory dependencies, coordination activities, approval timelines, launch integration considerations, and risks associated with achieving required operational or demonstration readiness milestones.

i. Security Compliance Approach: Description of the proposed security compliance approach, including applicable security requirements, cybersecurity considerations, protection of Government data, and planned evidence supporting security compliance.

j. External Interface Maturity and Interoperability Status: Updated assessment of external interface definitions and interoperability maturity associated with the proposed NEXUS service architecture. The assessment must identify the status of applicable Interface Control Documents (ICDs), interface standards implementation, interoperability validation activities, open interface issues, known constraints, and planned closure actions. The Contractor must identify any interfaces requiring additional coordination with NASA, mission users, commercial providers, launch providers, regulatory authorities, or other external stakeholders.

k. Ground Infrastructure Definition and Operational Support Approach: Description of the proposed ground infrastructure and operational support architecture required to execute, manage, monitor, secure, and maintain NEXUS service delivery. The discussion must include relevant ground stations, gateways, network operations capabilities, scheduling and resource management infrastructure, cybersecurity monitoring capabilities, cloud or data hosting environments where applicable, operational support systems, and continuity provisions. The Contractor must describe how the ground architecture supports service availability, interoperability, scalability, resiliency, and transition to sustained operations.

l. Resiliency and Fault Tolerance Approach: Updated description of resiliency, fault tolerance, redundancy, recovery, and continuity-of-operations approach supporting the proposed NEXUS service architecture. The description must identify key architectural features, operational concepts, backup capabilities, recovery timelines, autonomous or operator-assisted fault management approaches, and major resiliency risks. The Contractor must discuss how the proposed architecture supports continuity of service objectives in the presence of system anomalies, asset degradation, cyber events, communications disruptions, or loss of critical infrastructure elements.

m. Execution Schedule for CLIN 2: Proposed schedule for CLIN 2, including major milestones, decision points, long-lead activities, integration and test events, regulatory milestones, launch-related milestones, on-orbit demonstration activities, and critical path.

n. Transition-to-Service Approach: Description of the preliminary approach for transitioning from demonstration activities toward follow-on service delivery, including major readiness criteria and dependencies.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

o. Continuity of Service Operations Approach: Summary of the Contractor's approach to maintaining continuity of service during off-nominal conditions, including identification of credible disruption scenarios, high-level continuity strategies (e.g., redundancy, failover, alternate service delivery), service prioritization and recovery approach, key dependencies affecting continuity, and overall maturity of the continuity concept. Detailed continuity planning must be provided in NEXUS-DRD-010, Continuity of Service Operations Plan (CSOP).

p. Assembly, Integration, and Ground Test Approach: Description of the planned assembly, integration, verification, validation, and ground test approach supporting demonstration readiness and transition toward operational service capability. The description must include the overall integration strategy, major integration events, planned test environments, end-to-end interoperability testing approach, validation activities, verification dependencies, and use of simulation, emulation, digital environments, or representative operational configurations. The Contractor must identify critical integration risks, facility dependencies, test constraints, and planned approaches for demonstrating operational readiness and service performance.

q. Mission Assurance Approach: Proposed approach for Government mission assurance, interoperability protections, continuity support mechanisms, Government Purpose Rights, operational data rights, and any proposed strategic continuity constructs relevant to sustained service operations.

r. Intellectual Property and Data Rights Approach: Description of the proposed intellectual property, licensing, proprietary data handling, and Government data rights approach associated with the proposed NEXUS architecture, interfaces, software, operational data products, and supporting documentation. The description must identify any anticipated restrictions, limitations, or dependencies that could impact Government insight, interoperability, transition activities, operational sustainment, or future service competition considerations.

s. Open Issues and Government Decision Considerations: Identification of unresolved issues, assumptions requiring Government concurrence, decision points, requested clarifications, and recommended actions prior to proceeding into CLIN 2.

t. Post-Selection/Continuation Engagement Strategy: Proposed approach for post-selection engagement with NASA to support continued architecture maturation, demonstration execution, verification closure, operational readiness activities, transition planning, and continuity toward operational service capability. The discussion must describe the proposed insight/oversight model, coordination mechanisms, technical interchange approach, review support strategy, and planned Government engagement activities necessary to support successful continuation into subsequent NEXUS phases.

u. Presentation Package: A briefing package suitable for Government review boards or decision authorities. The presentation must summarize the written report and highlight decision-relevant information, including architecture, compliance posture, major risks, schedule, demonstration approach, and readiness to proceed into CLIN 2.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

v. Oral Presentation: The Contractor will provide an oral presentation of the CLIN 1 Design Outbrief Package to Government review participants, technical authorities, and decision makers. The oral presentation must utilize the Presentation Package described in section (u) and should communicate the Contractor's assessment of architecture maturity, integration readiness, technical risk posture, and readiness to proceed into system integration and ground test activities. The presentation must summarize key findings, accomplishments, major risks, open issues, remaining maturation activities, Government decision considerations, constraints, dependencies, and planned actions required to proceed into CLIN 2. The oral presentation should include a question-and-answer session with Government participants and must support Government assessment of architecture maturity and integration readiness.

15.4 **FORMAT**: Contractor format is acceptable. The submittal must include both a written report and a presentation package. The written report must be concise, decision-focused, and organized in a manner that supports Government assessment of readiness to proceed into CLIN 2. Appendices may include supporting technical details, data, analyses, trade studies, compliance matrices, risk tables, schedule details, and other substantiating information. Appendices must not be used in place of required substantive discussion in the main body of the report.

15.5 **MAINTENANCE**: This DRD is a point-in-time decision product. Updates are not required after submission unless requested by the Government to support clarification, decision-making, or resolution of open issues prior to CLIN 2 continuation.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-013**
3. **DATA TYPE**: 1
4. **DATE REVISED**:
5. **PAGE**: 1/3

6. **TITLE**: CLIN 2 Demonstration Readiness Package

7. **DESCRIPTION/USE**: To provide the Government with a concise, decision-focused written report and presentation package demonstrating the Contractor's readiness to execute the CLIN 2 on-orbit demonstration and supporting NASA's determination regarding continuation into CLIN 3. The package must document the final end-to-end system design, verified requirements compliance posture, demonstration and validation readiness, and execution capability, including risk posture, schedule, regulatory readiness, and operational preparedness.

   This DRD supports a Demonstration Readiness Review (DRR) and must provide sufficient evidence that the system is ready to proceed into demonstration execution with acceptable risk.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief**: Not applicable; **CLIN 2 Authorization to Proceed + 30 days**: Not applicable; **Demonstration & Integration Maturity**: Not applicable; **Demonstration Readiness Review**:: No later than 30 calendar days prior to the conclusion of CLIN 2 period of performance, or as specified in the contract. **Oral Presentation** must follow the delivery of the written package; **Demonstration Performance Validation Review**: Not applicable

12. **SUBMISSION FREQUENCY**: One-time submittal. Updates may be requested by the Government to support clarification, closure of open items, or final readiness determination.

13. **REMARKS**: The written report must be concise and decision focused. Appendices may contain supporting technical details, data, analyses, and substantiating material, but should not be used to avoid providing the required substantive discussion in the main body of the report. This DRD represents the final design and readiness state for demonstration execution and must reflect closure or disposition of all major design, integration, verification, and planning activities required to support on-orbit demonstration.

14. **INTERRELATIONSHIP**: NEXUS-DRD-001, Service Requirements Compliance Matrix, NEXUS-DRD-002, Service Demonstration & Validation Plan, NEXUS-DRD-003, Verification Closure Notices , NEXUS-DRD-004, External Interface Control Documents (ICDs), NEXUS-DRD-006, Service Transition Plan, NEXUS-DRD-010, Continuity of Service Operations Plan, NEXUS-DRD-012, CLIN 1 Decision Report and Presentation Package, and applicable contract paragraphs [TBD] related to verification and compliance demonstration.

DRD Continuation Sheet

TITLE: CLIN 2 Demonstration Readiness Package **DRD NO.**: **NEXUS-DRD-013**
DATA TYPE: 1 **PAGE**: 2/3

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The CLIN 2 Demonstration Readiness Package must provide sufficient information to demonstrate that the Contractor's system, operations, interfaces, verification, and supporting infrastructure are fully prepared to execute the on-orbit demonstration and meet NEXUS service objectives. The package must reflect the final system design, verified requirements compliance, validated demonstration plan, and readiness of all supporting elements, including launch, regulatory, security, interfaces, ground systems, and operations.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:
NEXUS-RQMT-001 *NEXUS Service Requirements Document*

15.3 **CONTENTS**: The CLIN 2 Demonstration Readiness Package must include, at a minimum, the following:

a. Executive Summary: Summary of system readiness, key accomplishments, residual risks, open issues, and Contractor's assessment of readiness to proceed with the on-orbit demonstration.
b. Final End-to-End System Architecture and Design Solution: Final description of the NEXUS service architecture, including space segment, ground segment, network/service delivery architecture, and all design updates since CLIN 1.
c. Final Requirements Compliance and Verification Status: Summary of final compliance with NEXUS SRD requirements, including verification status, completed VCNs, remaining open items (if any), and disposition plans. Detailed compliance data may be provided by reference to NEXUS-DRD-001, Service Requirements Compliance Matrix (SRCM).
d. Final Demonstration and System Validation Plan; Final approved plan for executing the on-orbit demonstration, including objectives, scenarios, success criteria, validation approach, and data collection methods.
e. Technical, Schedule, and Cost Risk Assessment: Updated assessment of all major risks, including mitigation status, residual risk, and impacts to demonstration execution and follow-on service.
f. Final Launch Services and Regulator Compliance Status: Description of launch readiness, licensing status, regulatory approvals, spectrum authorization, export control compliance, and any remaining regulatory dependencies.
g. Approved Security Compliance Approach: Final security posture, including implemented controls, compliance status, cybersecurity readiness, and protection of Government data and interfaces.
h. Final Hardware and Software Technology Readiness Assessment: Assessment confirming readiness of all hardware, software, and supporting systems for demonstration, including qualification status and integration readiness.
i. Final External Interface Definition: Summary of finalized interfaces, interface control status, interoperability readiness, ICD completion status, and interface verification results.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

j. Final Ground Infrastructure Definition and Operations Approach: Description of the operational ground systems, network infrastructure, mission operations capability (scheduling, service monitoring, data delivery, assumptions), and readiness to support demonstration execution.

k. .Final Resiliency and Fault Tolerance Approach: Summary of implemented resiliency, redundancy, fault management, and anomaly response capabilities supporting reliable demonstration operations.

l. Continuity of Service Operations Readiness: Summary of readiness to maintain continuity of service during demonstration, including validated contingency strategies, recovery approaches, dependencies, and alignment with the NEXUS-DRD-010, Continuity of Service Operations Plan.

m. Demonstration Execution Schedule: Final integrated schedule for the on-orbit demonstration, including major milestones, critical path, launch integration, on-orbit operations, and validation activities.

n. Final Transition-to-Service Approach: Description of the mature approach for transitioning from demonstration to service delivery, including readiness criteria, operational activation path, and dependencies.

o. Intellectual Property and Data Rights Approach: Final description of intellectual property, data rights, proprietary elements, and Government access consistent with contract requirements.

p. Open Issues and Government Decision Considerations: Identification of any remaining open issues, risks requiring Government awareness, decision points, or actions required prior to proceeding into CLIN 3.

q. Deviations and Waivers: Summary of all requested, approved, and pending deviations and waivers, including affected requirements or standards, rationale, approval status, associated impacts, mitigation measures, and any items requiring Government decision prior to proceeding into CLIN 3.

r. Presentation Package: A comprehensive briefing package supporting the Demonstration Readiness Review, summarizing system readiness, architecture, compliance status, risks, schedule, and demonstration execution approach.

15.4 **FORMAT**: Contractor format is acceptable. The submittal must include both a written report and a presentation package. The written report must be concise, structured, decision-focused, and organized in a manner that supports Government assessment of readiness to proceed into CLIN 3. Appendices may include supporting technical details, data, analyses, verification evidence, compliance matrices, risk matrices, schedule, interface details, and other substantiating information. Appendices must not be used in place of required substantive discussion in the main body of the report.

15.5 **MAINTENANCE**: This DRD is a point-in-time decision product. Updates are not required after submission unless requested by the Government to support clarification, decision-making, or resolution of open issues prior to CLIN 3 continuation.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-014**
3. **DATA TYPE**: 2
4. **DATE REVISED**:
5. **PAGE**: 1/3

6. **TITLE**: Monthly Program Status Report (MPSR)

7. **DESCRIPTION/USE**: To provide the Government with recurring, concise, and decision-oriented insight into Contractor program execution, including demonstration readiness, service capability maturation, schedule performance, mission integration progress, and readiness for transition to operational service. The Monthly Program Status Report (MPSR) and Integrated Master Schedule (IMS) updates, digital collaboration environment, and event-driven notifications collectively provide NASA with timely, actionable visibility to support capability readiness assessments, milestone acceptance, payment authorization, continuation decisions, and down-select determinations.

   Reporting emphasizes outcomes, execution status, and forward-looking insight, rather than detailed subsystem-level processes, and must enable continuous Government awareness of risks, dependencies, and performance trends.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: **Monthly Program Status Report (MPSR):** No later than the 10th business day of each month. **Integrated Master Schedule (IMS):** Submitted concurrently with each MPSR. **Oral Presentation** will coincide or follow the delivery of the report. **Event-Driven Notifications:** As specified in Section 15.3. **Digital Collaboration Environment Access:** Continuous, throughout contract performance.

12. **SUBMISSION FREQUENCY**: MPSR, IMS, and oral presentation: Monthly. Notifications: Event-driven. Digital access: Continuous. Updates may be requested by the Government to support clarification, closure of open items, or final readiness determination.

13. **REMARKS**: Reporting must be concise, decision-focused, and structured to provide clear Government insight into execution status, risks, and readiness. The Contractor should leverage digital tools and dashboards where practical to support continuous visibility, supplemented by formal monthly reporting. Subsystem-level details must be included only where directly relevant to program risk, schedule impact, demonstration success, service capability delivery, or Government awareness.

14. **INTERRELATIONSHIP**: NEXUS-DRD-001, Service Requirements Compliance Matrix, NEXUS-DRD-002, Service Demonstration and Validation Plan, NEXUS-DRD-004, Verification Closure Notices (VCNs), NEXUS-DRD-010, Continuity of Service Operations Plan (CSOP), NEXUS-DRD-012, CLIN 1 Design Outbrief Package, NEXUS-DRD-013, CLIN 2 Demonstration Readiness Package and applicable contract paragraphs [TBD] related to verification and compliance demonstration.

DRD Continuation Sheet

TITLE: Monthly Program Status Report (MPSR) **DRD NO.**: **NEXUS-DRD-014**
DATA TYPE: 2 **PAGE**: 2/3

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The Monthly Program Status Report (MPSR) must provide monthly and event-driven reporting that enables the Government to assess program health, execution progress, risks, dependencies, and readiness for demonstration and transition to operational service. Reporting must be structured to support timely decision-making, focusing on project-level execution and forward-looking insight.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:
NEXUS-RQMT-001 *NEXUS Service Requirements Document*

15.3 **CONTENTS**: The Monthly Program Status Report (MPSR) must include, at a minimum, the following:

a. Monthly Program Status Report (MPSR):
   1. Overall Program Health and Key Accomplishments - Summary of program status, major accomplishments during the reporting period, and overall health assessment.
   2. Progress Toward Demonstration Readiness - Status of progress toward Demonstration Readiness, including upcoming events, key milestones, and success criteria.
   3. Milestones and Critical Path Status - Status of major milestones, critical path activities, and any schedule risks or changes.
   4. Risk Assessment and Mitigation Status - Summary of top technical, regulatory, spectrum, mission integration, and programmatic risks, including mitigation status and residual impacts.
   5. Requirements Compliance Metrics and Status - Summary of compliance status, trends, and any significant gaps or risks to meeting NEXUS SRD requirements.
   6. Mission User Integration Status - Summary of mission user integration activities, key issues, and impacts to demonstration or service capability.
   7. Cross-Segment Dependencies - Identification of dependencies across space, ground, network, regulatory, and mission elements affecting relay service capability.
   8. Scalability to Sustained Service - Assessment of scalability toward sustained service, including identification of material gaps, constraints, or limiting factors.
   9. Issues and Government Awareness items - Identification of issues requiring Government awareness, support, or decision.

b. Integrated Master Schedule (IMS):
   1. Be provided in an industry-standard format (e.g., Microsoft Project, Primavera, or equivalent) and include.
      (1) Major milestones and critical path activities.
      (b) Logic ties and key dependencies, including regulatory dependencies.
      (c) Variance analysis against the approved baseline schedule.
   2. If any milestone is forecast to slip by more than **fifteen (15) calendar days**, the Contractor will:
      (a) Notify NASA within **five (5) business days**.
      (b) Provide:
         (1) Preliminary root cause assessment.
         (2) Mitigation or recovery plan.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

(3) Revised schedule forecast.
(4) Critical path impact assessment.

c. Digital Collaboration Environment - The Contractor will provide NASA with **read-only access** to a secure digital collaboration environment, where practical and consistent with Contractor processes, to support continuous visibility into program execution. At a minimum, the environment must include:
   1. Program performance dashboard.
   2. Milestone evidence packages and supporting data.
   3. Interface and integration artifacts.
   4. Version-controlled schedule updates.
   5. Service performance metrics (once available).

d. Event-Driven Notifications - The Contractor will notify NASA of any event that could materially affect program schedule, relay service capability, mission integration, or safety. Notifications must be submitted via the digital collaboration environment with email confirmation to the NASA team, unless otherwise directed. Notification timing must be:
   1. **Within 24 hours:** Safety hazards, mission-impacting anomalies, or service outages affecting demonstration or operations.
   2. **Within 48 hours:** Significant technical issues, regulatory delays, supply chain disruptions, or integration failures.
   3. **Within five (5) business days:** Forecast milestone slips greater than fifteen (15) calendar days, including root cause, mitigation plan, revised forecast, and critical impacts.

15.4 **FORMAT**: Contractor format is acceptable. The MPSR may be delivered as a narrative report, chart package, dashboard export, or combination thereof, provided it is concise, structured, and decision focused. Appendices may include supporting technical details, data, analyses, verification evidence, compliance matrices, risk matrices, schedule, interface details, and other substantiating information. Appendices should not be used in place of required substantive discussion in the main body of the report. The IMS must be provided in a standard scheduling tool format or Microsoft Excel. Digital collaboration tools may be used to supplement formal submissions.

15.5 **MAINTENANCE**: The MPSR and IMS must be updated and submitted monthly. Digital collaboration environment content must be maintained current throughout contract execution. Event-driven notifications must be provided as required to ensure timely Government awareness of significant events.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-015**
3. **DATA TYPE**: 2
4. **DATE REVISED**:
5. **PAGE**: 1/3

6. **TITLE**: CLIN 2 Demonstration Performance Validation Package (DPVP)

7. **DESCRIPTION/USE**: To provide the Government with a concise summary and results of the demonstration showing validation of NEXUS System capabilities. Detailed metrics must be provided for ground and space segments over the entire demonstration timeframe including availability data, failed contacts, and NEXUS system issues and outages. The review package must include for each user total operations forward/return time requested, scheduled, and accomplished, with data compiled and summarized for all users. Detailed demonstration data for individual SRD requirements should be provided to validate forward/return functional and performance requirements. Specific criteria prescribed for the demonstration should also be addressed with proper evidence of accomplishment during the demonstration. The Contractor must provide data package for review and present the data package orally.

   This DRD supports a Demonstration Performance Validation Review (DPVR) and must provide sufficient evidence that the system is capable of providing required NEXUS System Ka-Band service to legacy Government Users.

8. **OPR**: NEXUS 9. **DM**: ST30

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: **Written report** - approximately 30 calendar days after the completion of the minimum 30-calendar-day on-orbit performance measurement period. **Oral Presentation** will follow the delivery of the written report

12. **SUBMISSION FREQUENCY**: One-time submittal

13. **REMARKS**: The written report must be complete and accurate. Appendices may contain supporting technical details, raw data, analyses, and substantiating material, but should not be used to avoid providing the required substantive discussion in the main body of the report. This DRD represents the results of the Demonstration and provides validation of the NEXUS Ka-Band capabilities.

14. **INTERRELATIONSHIP**: NEXUS-DRD-001, Service Requirements Compliance Matrix, NEXUS-DRD-002, Service Demonstration & Validation Plan, Verification Closure Notices, NEXUS-DRD-004, External Interface Control Documents (ICDs), NEXUS-DRD-006, Service Transition Plan, NEXUS-DRD-010, Continuity of Service Operations Plan and applicable contract paragraphs [TBD] related to verification and compliance demonstration.

DRD Continuation Sheet

TITLE: CLIN 2 Demonstration Performance Validation Package (DPVP) **DRD NO.**: **NEXUS-DRD-015**

DATA TYPE: 2 **PAGE**: 2/3

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The CLIN 2 Demonstration Performance Validation Package must provide sufficient information to demonstrate that the Contractor's system, operations, interfaces, verification, and supporting infrastructure provided the capabilities and performance required to meet NEXUS service objectives.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:

NEXUS-RQMT-001 *NEXUS Service Requirements Document (SRD)*

15.3 **CONTENTS**: The CLIN 2 Demonstration Performance Validation Package must include, at a minimum, the following:

a. Executive Summary: Summary of system performance and Contractor's assessment of demonstration success in providing NEXUS Ka-Band service capabilities.
b. Demonstration Overview: Summary of the demonstration timeframe and duration, participating users, relay scheduling, ground and space segment configurations utilized during the demonstration, operational scenarios executed, significant operational events or anomalies. Specific criteria prescribed for the demonstration should also be addressed with proper evidence of accomplishment during the demonstration.
c. Service Requirements Performance Validation Results: Detailed measured functional and performance results validating applicable NEXUS SRD per NEXUS-RQMT-001 requirements. Supporting analysis products and qualitative datasets should be provided to support Government review and assessment of demonstration performance results.
d. Final Verification Closure Status: Summary of final verification compliance status against applicable NEXUS SRD requirements, including identification of requirements fully or partially verified through demonstration activities. Applicable NEXUS-DRD-003, Verification Closure Notices supporting demonstrated requirement verification closure must be submitted as part of the DPVP data package.
e. Final External Interface Definition: Summary of any required changes to NEXUS DRD-004, External Interface Control Documents.
f. Continuity of Service Operations Readiness: Summary of any changes to the NEXUS DRD-010, Continuity of Service Operations Plan based on demonstration.
g. Demonstration Execution As-Flown Timeline: As-flown timeline detailing ground and space segment configuration/maintenance, User planning and scheduling, and User forward/return services provided.
h. Risk Reduction: Identification of any risks that were reduced or retired based on the demonstration and final state of all NEXUS-related risks.
i. Final Transition-to-Service Approach Updates: Description of any changes to the approach for transitioning from demonstration to a mission-assured service delivery based on Demonstration execution. Updates to NEXUS DRD-006, Service Transition Plan and NEXUS DRD-008, Service Financial and Pricing Structure Definition as required.

DRD Continuation Sheet

TITLE: CLIN 2 Demonstration Performance Validation Package (DPVP) **DRD NO.**: **NEXUS-DRD-015**

DATA TYPE: 2 **PAGE**: 3/3

15. **DATA PREPARATION INFORMATION**:

j. Issues, Anomalies, and Lessons Learned: Detailed description of demonstration anomalies and operational issues encountered during demonstration execution with associated root-cause assessments and corrective actions taken. Documented lessons learned and recommended improvements.

k. Open Issues and Government Decision Considerations: Identification of any open issues, risks requiring Government awareness, decision points, or actions required prior to proceeding with NEXUS Ka-Band Full-Service capability.

15.4 **FORMAT**: Contractor format is acceptable and must include a written report and a presentation package. The presentation package should be complete, accurate, and organized in a manner that supports Government assessment of Demonstration success in providing NEXUS Ka-Band service capabilities. Appendices may include supporting technical details, raw data, analyses, verification evidence, compliance matrices, risk matrices, schedule, interface details, and other substantiating information.

15.5 **MAINTENANCE**: This is a one-time product. Updates are not required after submission unless requested by the Government to support clarification, decision-making, or resolution of open issues prior to contract continuation/completion.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-016**
3. **DATA TYPE**: 1
4. **DATE REVISED**:
5. **PAGE**: 1/3

6. **TITLE**: Organizational Conflict of Interest (OCI) Plan

7. **DESCRIPTION/USE**: The Plan will communicate the contractor's approach to identify and resolve OCIs. The contractor will be held accountable for identifying, dispositioning, and reporting OCIs during contract performance.

8. **OPR**: OP 9. **DM**: ST40

10. **DISTRIBUTION**: Distribution shall be as instructed by the Contracting Officer (CO)

11. **SUBMISSIONS**: Plan shall be submitted with the initial proposal

12. **SUBMISSION FREQUENCY**: As needed

13. **REMARKS**:

14. **INTERRELATIONSHIP**: NASA Federal Acquisition Regulation (FAR) Supplement (NFS) 1852.209-71, Limitation of Future Contracting, NFS 1852.237-72, Access to Sensitive Information and NFS 1852.237-73, Release of Sensitive Information.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The OCI Plan describes the contractor's comprehensive approach to identify, avoid, mitigate, neutralize, and report potential OCI issues, including conflicts described in the solicitation and those discovered during contract performance.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**:

FAR Subpart 9.5	*Organizational and Consultant Conflicts of Interest*
NFS 1809.500	*NASA Guide on Organizational Conflicts of Interest*

15.3 **CONTENTS**: The Organizational Conflict of Interest (OCI) Plan shall meet the requirements of FAR 9.5 and include the following:

a. Point of contact for OCI issues and reports.

b. Demonstrate an understanding of (1) OCI principles and (2) the full breadth of OCI issues and the types of harm that can result. The Plan at a minimum addresses the three primary types of OCIs (i.e., biased ground rules, unequal access to information, and impaired objectivity).

c. Define company roles, responsibilities, and procedures for (1) screening (i.e., identifying/recognizing, analyzing/evaluating, resolving, and reporting) existing and new business opportunities for actual/potential OCIs and (2) monitoring and reporting all potential/actual OCIs that arise, resolving conflicts, and reporting previously unidentified OCIs or potential OCIs to the Government.

DRD Continuation Sheet

TITLE: Organizational Conflict of Interest (OCI) Plan **DRD NO.**: **NEXUS-DRD-016**
DATA TYPE: 1 **PAGE**: 2/3

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

d. Describe how employees are notified of the Plan's requirements and how this notification will be documented. Establish and require entrance training for new employees, refresher training for existing employees, and exit training for departing employees. Describe how completion of this training will be documented, including a copy of any training certification template that the contractor will use to document that its employees have completed training.

e. Describe how the contractor will report breaches of the protective measures in the Plan to the contracting officer. Describe what processes the contractor will implement following any breach and indicate that final resolution of the corrective action must be approved by the contracting officer.

f. Identify any affiliated companies/entities (e.g., a parent company or a wholly owned subsidiary) and procedures for coordinating OCIs with such affiliated companies/entities.

g. Address the process for reporting all potential/actual OCIs that arise during performance of the contract. An OCI report shall include (1) a description of the conflict, (2) the plan for resolving the conflict, and (3) the benefits/risks to contract performance associated with plan approval/acceptance. Specific resolution strategies shall be appended to the Plan upon approval by the Government.

h. Explain how the contractor will flow down the provisions of this Plan to any subcontractor that may have a conflict with regard to performing the requirements of this contract. Discuss affected subcontractors' OCI program as it relates to this contract and specifically explain how affected subcontractors will identify, resolve, and report actual/potential OCIs associated with this contract.

i. Define organizational and employee sanctions for violations of established OCI procedures/requirements/ guidelines.

j. Include an assertion from the Offeror that to the best of its knowledge no OCIs exist currently, if applicable. Provide a list of all the prime's and proposed subcontractor(s)'s NASA contracts and subcontracts currently being performed and contracts performed within the last five years of the release of this solicitation, in order to provide the CO a better understanding of other NASA work performed by the Offeror that may give rise to an actual or potential conflict. For each prime contract and subcontract listed, the Offeror shall: (1) identify the contract number; (2) describe the scope of work in sufficient detail to ascertain the likelihood of a conflict with performance of this contract; and (3) discuss any conflicts that may arise from performance of the listed contracts and award of this contract.

k. The Offeror shall also list any non-NASA Federal contracts and subcontracts that it or its proposed subcontractors are currently performing or have performed in the five years preceding the release of the solicitation that may give rise to an OCI. For each and subcontract listed, the Offeror shall: (1) identify the contract by number and name; (2) identify the name, address and contact information of the customer(s); (3) describe the scope of work in sufficient detail to ascertain the likelihood of a conflict with performance of this contract; and (4) discuss any conflicts that may arise from performance of the listed contracts and award of this contract.

DRD Continuation Sheet

TITLE: Organizational Conflict of Interest (OCI) Plan **DRD NO.**: **NEXUS-DRD-016**
DATA TYPE: 1 **PAGE**: 3/3

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

l. For financial or other interests or relationships beyond Federal contracts or subcontracts that may give rise to an OCI, the Offeror shall (1) address the nature and extent of the interest(s) or relationship(s); (2) list any entity or entities involved in the interest(s) or relationship(s) and award of this contract.

m. The Offeror shall address how it will avoid, neutralize, or mitigate each potential OCI listed above. Sufficient information must be provided to allow a meaningful evaluation of the potential effect of the interest on the performance of the statement of work.

n. Include a requirement to update this plan as necessary to address specific OCIs. All updates to the plan must be approved by the contracting officer and the updates/changes must be incorporated in the contract to be effective.

o. Require periodic self-audits to ensure compliance with established OCI procedures/requirements/ guidelines.

p. Define records related to the OCI plan (e.g., training and audit records) that will be made available to the Government upon request. Note: The OCI Plan as outlined in paragraphs a through p above is not for the purpose of addressing other very important contractual obligations such as (1) the contractor's obligation to protect sensitive information in accordance with NFS 1852.237-72, Access to Sensitive Information, (2) the contractor's obligation to conduct business in an ethical manner in accordance with FAR 52.203-13, contractor's Code of Business Ethics and Conduct, and (3) the contractor's obligation to prevent personal conflicts of interest in accordance with FAR 52.203-16, Preventing Personal Conflicts of Interest.

q. In an appendix to the OCI Plan identify the strategy (e.g., mitigation, limitation on future contracting, etc.) for resolving each OCI that is either identified in the solicitation or created by the requirements of the solicitation/contract and explain the effect of such strategy on performance of the contract. If using a firewall, explain how these actions will operate to successfully address the conflict without adversely affecting performance of the contract. (Note: Specific plans to limit future competition are reflected in the clause at NFS 1852.209-71, Limitation of Future Contracting.)

15.4 **FORMAT**: Contractor format is acceptable. The electronic format shall be compatible with Microsoft Office.

15.5 **MAINTENANCE**: The contractor shall review the OCI Plan on an annual basis or as directed by the contracting officer to revise the OCI Plan if necessary. Revisions are subject to Contracting Officer approval and shall be incorporated by change page or complete reissue.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-017**
3. **DATA TYPE**: 1
4. **DATE REVISED**:
5. **PAGE**: 1/4

6. **TITLE**: Security Requirements for Unclassified IT Resources

7. **DESCRIPTION/USE**: To ensure that IT security requirements, including Cyber Supply Chain Risk Management (C-SCRM), are met during performance of this contract.

8. **OPR**: OCIO 9. **DM**: ST40

10. **DISTRIBUTION**: All deliverables required by this DRD, except for the C-SCRM plan, shall be submitted electronically to the CO, COR, and NASA Organization's Information System Security Officer (ISSO) (i.e., Security Officer). Approval will be provided by the ISSO. If the organization does not have an ISSO, approval will be provided by the NASA Information Owner. C-SCRM plans shall be submitted to and approved by the ICT/C-SCRM Service Element Lead at: agency-dl-ocio-cys-cp-scrm@mail.nasa.gov.

11. **SUBMISSIONS**: **Information System Security and C-SCRM Plan(s)**: For contractor-owned systems, due at the start of phase-in. Initial submission not required for existing, approved plans for Government-owned and Contractor-managed systems. For new Federal Information Systems, due with the delivery of the system.
Non-Federal System Certification: Prior to any transfer of NASA non-public information to the contractor, the contractor shall provide documentation of the certification of the non-federal system to the security officer of the NASA organization that owns the information (typically the organization responsible for the contract). If the organization does not have an ISO, the attention shall be provided to the NASA Information Owner.
Information on Employees in Sensitive Positions/Assignments Report: At the start of phase-in.
IT Security Point of Contact: At the start of phase-in.
IT Security Awareness Training: Training required prior to access to NASA information and systems.
IT Security Role Based Training: Foundational training is provided prior to performance of assigned role. Initial evidence showing completion due at the end of phase-in.

12. **SUBMISSION FREQUENCY**: **Information System Security Plan(s) and C-SCRM Plan**: As Required.
Non-Federal System Certification: Annually.
Information on Employees in Sensitive Positions/Assignments Report: Annually.
IT Security Point of Contact: As Required.
IT Security Awareness Training: Annual on anniversary date of initial training.
IT Security Role Based Training: Annual on anniversary date of initial training. Evidence of completion due annually.

13. **REMARKS**:

DRD Continuation Sheet

TITLE: Security Requirements for Unclassified IT Resources **DRD NO.**: **NEXUS-DRD-017**

DATA TYPE: 1 **PAGE**: 2/4

15. **INTERRELATIONSHIP**:

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: All contracts that purchase, lease, network to, or otherwise utilize covered articles, which includes Government-funded IT (as defined by the FAR) must comply with NASA IT Security and C-SCRM Requirements.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**: Most current versions of the following:

FAR 52.204-21	*Basic Safeguarding of Covered Contractor Information Systems*
FAR 52.204–29	*Federal Acquisition Supply Chain Security Act Orders-Representation and Disclosures*
FISMA 2014	*Federal Information Security Modernization Act 2014*
NFS 1852.240-76	*Security Requirements for Unclassified IT Resources (DEVIATION PCD 26-03)*
NFS 1852.226-73	*Major Breach of Safety or Security (FEB 2026)*
NFS 1852.237-72	*Access to Sensitive Information (DEVIATION DEC 2025)*
NFS 1852.237-73	*Release to Sensitive Information (DEVIATION DEC 2025)*
NIST SP 800-171	*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
NIST SP 800-53	*Security and Privacy Controls for Information Systems and Organization*
NIST SP 800-161	*Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
NPR 1382.1	*NASA Privacy Procedural Requirements*
NPD 2810.1	*Information Security Policy*
NPR 2810.1	*Security of Information and Information Systems*
NPR 2810.7	*Controlled Unclassified Information*
NPR 7120.7	*NASA Information Technology Program and Project Management Requirements*
OMB Circular A-130	*Management of Federal Information Resources*

15.3 **CONTENTS**: The Federal Information Security Modernization Act (FISMA) and Executive Branch policy require external providers that process, store, or transmit federal information or operate information systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies.

DRD Continuation Sheet

TITLE: Security Requirements for Unclassified IT Resources **DRD NO.**: **NEXUS-DRD-017**

DATA TYPE: 1 **PAGE**: 3/4

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

a. Information System Security Plan (i.e., System Security Plan, IT Security Plan, or Security Plan): When the contractor is operating a Federal Information System (FIS) on behalf of NASA or is providing a FIS in the execution of this contract, that system must have an Information System Security Plan in accordance with NIST Special Publication (SP) 800-53, "Security and Privacy Controls for Information Systems and Organizations" at the revision number required at the issuance of the contract. This plan and supporting documents shall be entered into the NASA cybersecurity system of record pursuant to Authorization to Operate (ATO) requirements set forth in NASA Policy Directive 2810.1, "NASA Information Security Policy" and NASA Procedural Requirement (NPR) 2810.1, "Security of Information and Information Systems." The FIS security plan and ATO must be in place before any system may operate in the NASA environment.

b. Non-Federal System Security Certification: When the contractor will receive, process, store or transmit NASA non-public information, especially Controlled Unclassified Information (CUI) including Personally Identifiable Information (PII) on a non-federal system (e.g., the contractor's corporate system) the system must meet the requirements for data protections detailed in NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." This documentation may take the form of:

1. A third-party review/audit certifying that the non-federal system meets the requirements of NIST SP 800-171 or equivalent standard of information protection, such as the ISO 27001 standard.
2. A certification from another federal agency such as the DOD Cybersecurity Maturity Model Certification (CMMC) Level 2.

c. Incident Notification: The contractor shall report immediately upon notification any incident involving NASA information on nonfederal (contractor) systems to SOC@nasa.gov.

d. IT Security Point of Contact: The contractor shall identify a point of contact that NASA may reach in its attempt to address IT and cybersecurity issues. The point of contact shall have the authority to ensure the immediate notification of the NASA Security Operations Center of any incident involving NASA information.

e. IT Security Awareness Training: Contractor employees subject to this contract, defined as those requiring physical access to NASA facilities or electronic access to NASA systems, shall complete the NASA approved IT Security Awareness Training annually. NASA Cybersecurity and Privacy Awareness training is available through the SATERN online system and must be completed prior to access to NASA information and systems. Completion of the training is tracked automatedly by NASA and must recur each year by the anniversary of the initial training as a condition of continued access. Cybersecurity and Privacy training is updated throughout the year as needed, so there is no defined training period.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

f. IT Security Role Based Training: Contractor employees subject to this contract shall complete NASA's Foundational IT Security Training in SATERN related to the following role-based functions prior to performing the role

1. IT Security Manager.
2. Information System Owner (ISO).
3. Information System Security Officer (ISSO).
4. Information System Security Engineer (ISSE).

It is highly recommended, but not required, that Contractor employees complete advanced role-based training every other year following completion of the initial training provided by NASA. This training is also provided by NASA but may be fulfilled externally. If fulfilled externally, the Contractor shall provide the "External Role-Based Training Validation Form" to the center CISO. The process for completing this form and receiving credit may be found at: External RBT Validation Form (sharepoint.com).

g. Information on Employees in Sensitive Position(s)/Assignments Report: The Information on Employees is Sensitive. IT Security (ITS) Positions/Assignments Report shall provide information annually for personnel screening as required by NPR 2810.1(series), and NPR 1600.1 on position risk.

h. Cyber Supply Chain Risk Management (C-SCRM) Plan: NIST defines C-SCRM as a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. A C-SCRM plan, consistent with the recommended template in NIST SP 800-161, Section 3.1 shall be delivered prior to the processing, transmission, or storage of non-public NASA information in performance of the contract.

15.4 **FORMAT**: Unless otherwise directed, the data requested in this DRD shall be delivered to the Government in soft-copy via an electronic transfer mechanism (e.g., electronic mail, flash drive, or file transfer protocol) in a format readable by a Government device utilizing the standards in NASA-STD-2804, "Minimum Interoperability Software Suite."

15.5 **MAINTENANCE**: Information System Security Plan(s) shall be kept up to date as changes to the baseline configuration of the system(s) occur. Non-Federal System Certifications shall be maintained annually or per the certifying body's standard. Information on Employees in Sensitive Positions/Assignments Report shall be maintained annually. IT Security Point of Contact shall be kept up to date as changes occur. Evidence of completion of IT Security Role Based Training is due annually. C-SCRM plans shall be kept up to date as changes occur to organizational C-SCRM processes, policies, and procedures, and/or, new components are introduced.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-018**
3. **DATA TYPE**: 1
4. **DATE REVISED**:
5. **PAGE**: 1/5

6. **TITLE**: Demonstration Integration & Maturity Presentation Package

7. **DESCRIPTION/USE**: To provide the Government with a concise, decision-focused written report and presentation package demonstrating the Contractor's architecture maturity, integration readiness, and preparedness to proceed into system assembly, integration, verification, validation, and ground test activities supporting the NEXUS demonstration.

   The package will document the maturity of the end-to-end service architecture, technical baseline status, interface readiness, verification and validation planning maturity, integration strategy, risk posture, and readiness of supporting infrastructure necessary to initiate formal integration and test activities.

   This DRD supports the Demonstration & Integration Maturity milestone and provides the Government with sufficient information to assess whether the proposed NEXUS solution has achieved an acceptable level of technical maturity and integration readiness to proceed into system integration and ground testing with acceptable risk.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination

11. **SUBMISSIONS**: Demonstration Integration & Maturity Milestone; submit no later 30 calendar days prior or as otherwise specified by the contract. **Oral Presentation** must follow the delivery of the package.

12. **SUBMISSION FREQUENCY**: One time submittal. Updates may be requested by the Government to support clarification, risk resolution, or readiness determination.

13. **REMARKS**: This DRD supports Government assessment of architecture maturity and readiness to begin formal systems integration and ground test activities. This package should be concise, complete, and structured to support Government milestone review and approval activities. The Demonstration Integration & Maturity Presentation Package is a Type 1 data item subject to Government review and approval. The Contractor may summarize and reference supporting DRDs, analyses, models, schedules, compliance products, interface documentation, and design artifacts where appropriate. Detailed subsystem-level information should be included only where necessary to support assessment of integration readiness, technical maturity, or risk.

15. **INTERRELATIONSHIP**: NEXUS-DRD-001, Service Requirements Compliance Matrix; NEXUS-DRD-002, Service Demonstration & Validation Plan; NEXUS-DRD-003, Verification Closure Notices; NEXUS-DRD-004, External Interface Control Documents; NEXUS-DRD-005, Security Architecture Definition; NEXUS-DRD-006, Service Transition Plan; NEXUS-DRD-011, Verification/Validation Compliance Report; NEXUS-DRD-012, CLIN1 Design Outbrief Package; NEXUS-DRD-013, CLIN 2 Demonstration Readiness Package; and applicable contract paragraphs [TBD].

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: This Demonstration Integration & Maturity Presentation Package must provide the Government with sufficient information to determine whether the Contractor's architecture, interfaces, verification approach, integration plan, facilities, personnel, tools, and supporting infrastructure have matured to a level appropriate for initiation of system integration and ground testing activities. This package must emphasize technical maturity, interface readiness, integration readiness, verification and validation readiness, risk posture, and execution credibility rather than detailed design implementation. The level of detail should be sufficient to support Government assessment of integration readiness, identification of remaining technical and operational risks, and determination of that the Contractor is ready to proceed into formal assembly, integration, and test activities.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**: Most current versions of the following:

NEXUS-RQMT-001 *NEXUS Service Requirements Document*

15.3 **CONTENTS**: The Demonstration Integration & Maturity Presentation Package must include, at a minimum, the following:

a. Executive Summary: A concise summary of the overall architecture maturity assessment, integration readiness status, major accomplishments since the previous milestone, key risks and open issues, and the Contractor's assessment of readiness to proceed into system integration and test activities.

b. End-to-End Architecture Maturity: Description of the current architecture baseline, major architecture elements, status of architecture definition and allocation, design maturity, significant design trades completed, and remaining architecture maturation activities necessary to support integration and test readiness.

c. Requirements Compliance and Verification Maturity: Assessment of current requirements compliance status, verification planning maturity, validation planning maturity, verification closure status, and any open compliance issues, including planned resolution activities.

d. Interface Maturity and Integration Readiness: Assessment of the status and maturity of internal and external interfaces, Interface Control Document (ICD) maturity, interface verification strategy, interoperability readiness, and any open interface issues and planned closure activities.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

e. Assembly, Integration, and Ground Test Approach: Description of the integration philosophy and strategy, planned integration flow, major integration events, ground test strategy, end-to-end test approach, Test-Like-You-Fly (TLYF) implementation approach and any approved exceptions, and the criteria for successful integration and test completion.

f. Verification and Validation Readiness: Assessment of the status of verification and validation products, readiness of verification and validation procedures and success criteria, readiness of data collection and analysis methods, verification and validation execution schedule, and overall readiness to begin formal verification and validation activities.

g. Integration and Test Environment Readiness: Assessment of test facility readiness, ground system readiness, network and communications infrastructure readiness, emulator, simulator, and digital environment readiness, cybersecurity readiness supporting integration and test activities, operational support capability readiness, and any remaining integration environment constraints.

h. Technical Performance: Assessment of current technical performance, performance margin status, resource utilization, and any performance limitations or constraints that could affect integration readiness or demonstration objectives.

i. Technology and Design Maturity: Assessment of critical technology maturity, remaining technology and design maturation activities, qualification and certification status where applicable, and the impact of technology maturity on integration and test readiness.

j. Integration Risks: Assessment of technical integration risks, interface risks, verification and validation risks, schedule risks, facility and infrastructure risks, regulatory risks affecting integration readiness, mitigation plans and closure strategies, and the resulting residual risk posture.

k. Integrated Schedule: Assessment of the integration and test master schedule, major milestones and decision points, critical path activities, long-lead dependencies, and overall schedule confidence.

l. Personnel and Organizational Readiness: Description of the integration team organization, roles and responsibilities, staffing readiness, readiness of key partners and suppliers as applicable, and the coordination and governance approach supporting integration and test execution.

m. Open Issues and Government Decision Considerations: Identification of unresolved issues requiring Government awareness, required Government decisions, assumptions requiring Government concurrence, constraints requiring Government awareness, and recommended Government actions necessary prior to initiation of integration and test activities.

n. Readiness Declaration: A formal Contractor assessment of integration readiness status, major strengths, residual risks, and recommendation regarding proceeding into system integration and ground testing.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

o. Regulatory Compliance Readiness: Assessment of regulatory compliance readiness sufficient to support planned integration, ground test, demonstration, and service implementation activities. The assessment must identify applicable regulatory, licensing, authorization, certification, and coordination requirements; status of regulatory compliance activities; status of radio frequency spectrum coordination and licensing activities; status of launch-related approvals where applicable; status of cybersecurity authorizations including Authority to Connect (ATC), Authority to Operate (ATO), or equivalent approvals; export control compliance status; status of commercial, international, interagency, and third-party coordination activities; regulatory dependencies, assumptions, constraints, and external approvals; open regulatory issues and planned resolution activities; overall regulatory readiness; and planned regulatory milestones and activities required prior to Demonstration Readiness Review (DRR) and demonstration execution.

p. Presentation Package: A briefing package suitable for Government review boards, technical authorities, and decision makers. The presentation package should summarize the information contained in sections (a through o) and provide sufficient detail to support Government assessment of architecture maturity, integration readiness, technical risk posture, and readiness to proceed into system integration and ground test activities. The presentation must communicate key accomplishments, major risks, open issues, Government decision considerations, remaining maturation activities, and planned actions necessary to achieve Demonstration Readiness Review (DRR) entry criteria. The presentation package may include charts, graphics, schedules, architecture diagrams, readiness assessments, risk summaries, compliance status, interface status, and other visual materials necessary to effectively communicate technical maturity and integration readiness and should be suitable for oral presentation and subsequent Government review and archival purposes.

q. Oral Presentation: The Contractor will provide an oral presentation of the Demonstration Integration & Maturity Presentation Package to Government review participants, technical authorities, and decision makers. The oral presentation must utilize the Presentation Package described in section p and should communicate the Contractor's assessment of architecture maturity, integration readiness, technical risk posture, and readiness to proceed into system integration and ground test activities. The presentation must summarize key findings, accomplishments, major risks, open issues, remaining maturation activities, Government decision considerations, constraints, dependencies, and planned actions required to achieve Demonstration Readiness Review (DRR) entry criteria and must include the Contractor's assessment of readiness to proceed into system integration and ground testing. The oral presentation should include a question-and-answer session with Government participants and must support Government assessment of architecture maturity and integration readiness.

DRD Continuation Sheet

TITLE: Demonstration Integration & Maturity Presentation Package

DRD NO.: **NEXUS-DRD-018**

DATA TYPE: 1

PAGE: 5/5

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

15.4 **FORMAT**: Unless otherwise directed, the data requested in this DRD must be delivered to the Government in soft-copy via an electronic transfer mechanism (e.g., electronic mail, flash drive, or file transfer protocol) in a format readable by a Government device utilizing the standards in NASA-STD-2804, "Minimum Interoperability Software Suite."

15.5 **MAINTENANCE**: This DRD is a point-in-time milestone product. Updates are not required following completion of the Demonstration & Integration Maturity review unless requested by the Government to support clarification, closure of open actions, or readiness determination prior to initiation of system integration and ground test activities.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-019**
3. **DATA TYPE**: 2
4 **DATE REVISED**:
5. **PAGE**: 1/4

6. **TITLE**: Integrated Master Schedule (IMS)

7. **DESCRIPTION/USE**: To provide the contractor's time-phased plan, current status, key milestones, major program activities, milestones, demonstrations, service readiness activities, and dependencies necessary to accomplish contract objectives. This schedule will be used to provide management insight into contractor status, potential problem areas, schedule status, milestone achievement, and identification of potential impacts to contractual commitments, demonstration readiness, service capability maturation, and IOC transition.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per Contracting Officer's letter

11. **SUBMISSIONS**: Preliminary IMS is due with proposal. The first submission is due between 60 and 90 calendar days after the Authority to Proceed (ATP), pending government approval.

12. **SUBMISSION FREQUENCY**: Monthly, by the 12th working day after the close of the contractor's accounting month.

13. **REMARKS**: The schedule will be baselined after ATP as agreed to by both parties and not to exceed 90 days after ATP. The IMS reporting levels, and frequency shall be in accordance with the Contract Work Breakdown Structure and contract provisions. Reference is made to NPR 7120.5, *NASA Space Flight Program and Project Management Requirements* (Current Revision), NPR 7120.7, *NASA Information Technology Program and Project Management Requirements* (Current Revision), NPR 7120.8, *NASA Research and Technology Program and Project Management Requirements* (Current Revision), and *NASA Schedule Management Handbook* available at http://www.nasa.gov/evm/handbooks. These references are provided for schedule management guidance only and do not impose additional contractual program management, reporting, or development process requirements beyond those specified herein.

14. **INTERRELATIONSHIP**: NEXUS-DRD-012, CLIN1 Design Outbrief Package, NEXUS-DRD-013, Demonstration Readiness Package and NEXUS-DRD-014, Monthly Program Status Report.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The IMS provides data for the assessment of contractual milestone achievement, schedule status, readiness activities, and potential impacts to demonstration execution and service transition objectives. The IMS is intended to provide Government insight into contractual milestone achievement, demonstration readiness, service capability maturation, and IOC transition planning. The IMS is not intended to prescribe contractor internal management processes or require disclosure of proprietary execution details beyond those necessary to assess contractual performance and readiness.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**: None

15.3 **CONTENTS**: The IMS shall include tasks necessary to accomplish the total scope of work as defined in the contract statement of work and the WBS. The IMS shall be created and maintained in a management software tool that supports automated time phasing of tasks and Critical Path Method (CPM) functionality. The level of detail of data provided within the IMS shall be established by the responsible NASA Project Management Office.

a. Minimum requirements for the IMS content:

1. The IMS shall include the contractual milestones, target/control milestones (where applicable), key subcontract milestones, discrete tasks/activities, current progress accomplishments, established baseline and current schedule dates, and key Government Furnished Property (GFP) and Government Furnished Equipment (GFE). Tasks shall be at a level of detail to allow for discrete progress measurement and visibility into the overall development flow, which typically includes service development, integration, verification, validation, demonstration preparation, regulatory activities, security authorization activities, operational readiness activities, and service transition activities. (Note: Task/milestone titles shall be clear, concise, non-repetitive, and reflect the scope and output (i.e.: deliverable) so that the task content can be understood as standalone data without its associated summary level-task also being shown.)
2. The IMS shall be an integrated, logically driven schedule that defines the relationships and dependencies among major contractual milestones, readiness activities, demonstrations, service capability maturation activities, and transition to operational service. Schedule logic shall be sufficient to support identification and preliminary analysis of critical path and all near (secondary) critical paths whose total slack (float) values are within 10 working days or less of the primary critical path, schedule drivers, and potential impacts to contractual requirements.
3. The IMS shall identify external dependencies, subcontractor activities, supplier deliveries, and partner commitments that could affect contractual milestones, demonstration readiness, service capability delivery, or transition to operational service.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

4. The IMS shall reflect accurate schedule progress and adhere to the following requirements: 1) Forecast start and forecast finish dates shall not be earlier than the current schedule status date. 2) Actual start and actual finish dates shall be recorded and not be later than the current schedule status date. 3) Tasks that have actual starts, but are not yet complete, shall reflect the most accurate expected forecast finish date.
5. The IMS shall have traceability to the approved WBS, Integrated Master Plan (IMP) (if applicable), subcontractor activity, and the Statement of Work. This traceability shall be accomplished by using data fields provided within the scheduling tool.
6. The IMS shall identify significant schedule constraints that materially affect contractual milestones or critical path analysis.
7. The IMS shall clearly identify tasks that contain risks and associated mitigation activities that could affect contractual milestones, demonstration readiness, service capability delivery, regulatory approvals, security authorization, or IOC transition.
8. The IMS shall also clearly identify schedule margin, to include management reserve, associated with major contractual milestones, demonstrations, and IOC transition activities.
9. The IMS shall contain the necessary calendars that accurately define working and nonworking time periods or other information that may impact the schedule.

b. The IMS shall be reported in four sections, as outlined below. Data included in the following deliverables shall be either extractions from or consistent with the automated logic network database. All data contained in the sections shall be consistent, progressed monthly, and based on the same cutoff date.

1. Summary Master Schedule – Top level, Gantt-type summary document arranged by WBS that reflects all contract and controlled milestones, major program/project phases (i.e., CLIN milestones, architecture maturity reviews, verification milestones, authority to connect, demonstration readiness milestones, demonstration execution, service transition milestones, IOC readiness milestones) and all end item deliveries. It shall reflect, either by manual creation or by automated summarization, a vertically integrated rollup of intermediate and detailed schedule data.
2. Detailed IMS Logic Network Schedule – The IMS shall provide a logically linked schedule identifying major contractual milestones, dependencies, critical paths, and schedule drivers associated with demonstration readiness, service capability delivery, and IOC transition. The schedule shall provide sufficient detail to support Government assessment of schedule status and readiness without prescribing contractor internal management practices.

15. **DATA PREPARATION INFORMATION (CONTINUED)**:

3. On an as-directed basis by NASA, the contractor shall conduct a probabilistic Schedule Risk Assessment (SRA) report. Analysis and discussion pertaining to SRA results will be reported in Format 5. The SRA will predict the probability of meeting the scheduled completion dates contained within the IMS. The SRA assessment shall be accomplished using a standard probabilistic management tool with monte-carlo functionality. Three-point duration estimates (minimum, maximum, and most likely) will be used in conducting the SRA. Three-point estimates shall be ascertained individually for those tasks that are identified as part of the project critical path, or near critical secondary paths, or tasks that have been identified as high-risk within the contractor's risk management system. All other remaining tasks within the IMS may have three-point estimates applied either individually or globally, as long as they are applied consistently across the entire IMS and the process is documented within the contractor's schedule management plan/process.
4. Contractor IMS Analysis and Assessment Discussion: The IMS analysis and assessment report shall address the following:
   (a) Critical Path Report. Critical Path reporting shall be an extract from the IMS Logic Network Database and include all discrete tasks and milestones that make up the longest path sequence to the designated project completion event or final contract delivery. This report shall also include identification and analysis of all primary and secondary critical path(s) and major schedule drivers affecting contractual milestones and readiness objectives.

   If requested by NASA, this report will also include detailed driving path information to selected contract or major project milestones/events. (NOTE: If driving paths are identified through the use of assigned task constraints (limited or fixed start/finish dates) within the IMS, then it shall be understood by the contractor that those constraints shall also be removed from the IMS network after identification and analysis of driving paths are complete. Constraints that are left within the IMS unnecessarily will hinder or prevent accurate project critical path identification and analysis.)
   (b) Contractor Schedule Assessment Discussion. The Contractor Schedule Assessment shall provide a narrative assessment of schedule status, major accomplishments, milestone performance, emerging schedule risks, critical path changes, significant forecast changes, and recovery actions associated with contractual commitments, demonstration readiness, service capability delivery, and IOC transition. The assessment shall also include a scheduled health check based on industry standards and best practices.

15.4 **FORMAT**: Submission of IMS deliverables shall be by electronic media. Electronic media submittals shall be provided in native format or mutually agreed electronic formats suitable for Government review.

15.5 **MAINTENANCE**: Changes shall be incorporated by complete reissue.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.**: 1916 **ISSUE**: RFP
2. **DRD NO.**: **NEXUS-DRD-020**
3. **DATA TYPE**: 2
4 **DATE REVISED**:
5. **PAGE**: 1/4

6. **TITLE**: Radio Frequency Link Margin and Dynamic Link Budget Analysis Report (RF-LMDBAR)

7. **DESCRIPTION/USE**: To provide the Government with the technical basis to assess whether the proposed NEXUS architecture can satisfy applicable NEXUS Service Requirements Document (SRD) radio frequency (RF) performance requirements under both static worst-case conditions and dynamic operational conditions throughout the proposed service volume.

   The report shall document RF link margin analyses, dynamic link budget analyses, modeling assumptions, performance sensitivities, limiting cases, and traceability to applicable SRD requirements. The report shall enable the Government to assess RF performance feasibility, identify performance limitations and risks, evaluate margin posture, and understand dependencies associated with achieving required service performance during demonstration and operational service delivery.

8. **OPR**: NEXUS 9. **DM**: ST40

10. **DISTRIBUTION**: Per program/project/activity determination.

11. **SUBMISSIONS**: **Proposal Submission**: Preliminary RF Link Margin and Dynamic Link Budget Analysis supporting the proposed architecture and demonstrating expected compliance with applicable SRD RF performance requirements. **Verification and Validation Compliance Review:** Not applicable; **CLIN 1 Design Outbrief (Vendor Down Select)**: Updated RF link margin and dynamic link budget analysis reflecting architecture maturation, updated design parameters, and refined performance assumptions; **CLIN 2 Authorization to Proceed (ATP) + 30 Days**: Updated analysis, design parameters, and refined performance assumptions; **Demonstration & Integration Maturity Milestone**: Updated analysis, design parameters, and refined performance assumptions; **Demonstration Readiness Review (DRR)**: Updated demonstration-ready analysis; **Demonstration Performance Validation Review**: Final update, as required, incorporating as-flown or best-available performance data.

12. **SUBMISSION FREQUENCY**: As needed

13. **REMARKS**: This DRD supports Government assessment of RF performance feasibility, architecture maturity, requirements compliance, and demonstration readiness. The analysis shall be sufficiently detailed to enable independent Government understanding of RF performance assumptions, margin posture, sensitivities, and performance limitations. This DRD is a Type 2 data item subject to Government review and approval by exception. The Contractor may utilize commercially available tools, proprietary tools, analytical models, simulation environments, or other accepted engineering methods. Detailed proprietary implementation information is not required provided sufficient information is supplied to support Government understanding of analysis results and conclusions.

14. **INTERRELATIONSHIP**: NEXUS-DRD-001, Service Requirements Compliance Matrix; NEXUS-DRD-002, Service Demonstration & Validation Plan; NEXUS-DRD-004, External Interface Control Documents; NEXUS-DRD-011, Verification/Validation Compliance Report; NEXUS-DRD-012, CLIN 1 Design Outbrief Package; NEXUS-DRD-013, CLIN 2 Demonstration Readiness Package; and NEXUS-RQMT-001, NEXUS Service Requirements Document.

15. **DATA PREPARATION INFORMATION**:

15.1 **SCOPE**: The Radio Frequency Link Margin and Dynamic Link Budget Analysis Report (RF-LMDBAR) shall provide quantitative analyses demonstrating the expected RF performance of the proposed NEXUS architecture throughout the proposed service volume. The report shall evaluate both static worst-case conditions and dynamic operational conditions and shall identify assumptions, sensitivities, limiting cases, performance margins, and any conditions affecting compliance with applicable SRD requirements. The report shall support Government assessment of architecture feasibility, demonstration readiness, and expected service performance and shall identify any RF performance areas requiring additional maturation, mitigation, operational constraints, or design assumptions.

Government assessment of architecture feasibility, demonstration readiness, and expected service performance and shall identify any RF performance areas requiring additional maturation, mitigation, operational constraints, or design assumptions.

15.2 **APPLICABLE DOCUMENTS/CLAUSES**: Most current versions of the following:

NEXUS-RQMT-00	*NEXUS Service Requirements Document*
NASA-STD-2804	*Minimum Interoperability Software Suite*

15.3 **CONTENTS**: The Radio Frequency Link Margin and Dynamic Link Budget Analysis Report (RF-LMDBAR) must include, at a minimum, the following:

a. Executive Summary: Summary of analysis objectives, major findings, RF performance conclusions, margin posture, challenged requirements, key assumptions, and overall assessment of expected compliance with applicable SRD RF requirements.

15. **DATA PREPARATION INFORMATION (CONTINUED)**

b. RF Architecture Overview: Description of the analyzed RF architecture, including relevant space segment, ground segment, user segment, frequencies, bandwidths, antenna configurations, waveform assumptions, and service volume definition.

c. Static Link Margin Analysis: Static RF link margin analyses demonstrating compliance with applicable SRD requirements under worst-case conditions. The analysis shall include, as applicable, spreading loss, implementation loss, system noise temperature, antenna efficiency, axial ratio effects, polarization losses, pointing error losses, slant range effects, atmospheric losses, EIRP assumptions, G/T assumptions, orbital geometry effects, and other significant contributors to RF performance.

d. Dynamic Link Budget Analysis: Dynamic RF link budget analyses evaluating expected performance across representative user trajectories, relay trajectories, operational geometries, and service volume conditions. The analysis shall identify expected performance variation over time and throughout the proposed service volume and shall identify any performance limitations, operational constraints, or sensitivity conditions.

e. SRD Traceability: Mapping of each analysis case, scenario, or performance assessment to the applicable NEXUS SRD RF requirement(s), including identification of associated requirement identifiers and compliance conclusions.

f. Assumptions and Input Parameters: Description of all modeling assumptions, analysis tools, trajectories, service volume definitions, antenna assumptions, RF parameters, margin assumptions, user assumptions, ground architecture assumptions, environmental assumptions, operational assumptions, and limiting cases utilized in the analysis.

g. Challenged or Marginal Requirements: Identification of any SRD RF requirement that is challenged, marginally met, conditionally met, dependent upon specific assumptions, or otherwise sensitive to design, operational, environmental, or performance uncertainties. The discussion shall identify contributing factors, impacts, assumptions, operational constraints, and planned mitigation approaches.

h. Sensitivity and Limiting Case Evaluation: Evaluation of significant performance sensitivities, limiting cases, worst-case operating conditions, and major performance drivers affecting RF margin or link performance.

i. Demonstration and Operational Implications: Assessment of how RF performance assumptions, margins, and limitations affect demonstration execution, validation activities, service availability, service coverage, operational constraints, and transition to operational service.

j. CLIN 2 Final/As-Built Analysis Update: Updated RF link margin and dynamic link budget analyses utilizing final design parameters, measured or best-available antenna patterns, final EIRP values, final G/T values, trajectory assumptions, ground architecture definition, user-service assumptions, and demonstration-ready or as-built system characteristics.

15. **DATA PREPARATION INFORMATION (CONTINUED)**

15.4 **FORMAT**: Unless otherwise directed, the data requested in this DRD must be delivered to the Government in soft-copy via an electronic transfer mechanism (e.g., electronic mail, flash drive, or file transfer protocol) in a format readable by a Government device utilizing the standards in NASA-STD-2804, "Minimum Interoperability Software Suite. The report may include narrative discussion, tables, charts, plots, coverage maps, dynamic performance visualizations, trajectory analyses, sensitivity analyses, margin summaries, and other engineering products necessary to support Government understanding of RF performance. Electronic formats that support Government review and independent examination of results are preferred. Supporting analytical data files may be provided as appendices or supplemental attachments.

15.5 **MAINTENANCE**: This DRD shall be maintained current throughout CLIN 2. Updates shall reflect architecture changes, updated RF performance assumptions, revised trajectories, measured performance data, demonstration configuration changes, and other factors affecting RF performance conclusions. Changes and updates shall be submitted in accordance with the schedule specified in Item 12 or as requested by the Government. Significant changes affecting expected SRD RF compliance, link margin posture, service volume coverage, or demonstration readiness shall be identified and reported in the next scheduled update.