

ATTACHMENT D

CONTRACT DATA REQUIREMENTS LIST

**National Aeronautics and Space Administration
Information Technology Procurement Office**

DOCUMENT CHANGE LOG

DRD No.	DRD Title	Revision	Date
2	AbilityOne Reporting		3.2024
3	Cybersecurity-Supply Chain Risk Management (C-SCRM) Plan	Initial Submission: The plan shall be submitted no later than 60 calendar days after contract award date.	6.2024
4	C-SCRM Incident Reporting		4.2024
5	Climate Change Risk Management Plan		4.2024

INTRODUCTION

This document defines the requirements for contractual data to be delivered by the contractor to the Government. The data requirements are set forth in each Data Requirements Description (DRD) and shall govern that data required by the contract. The contractor shall furnish data defined by the DRDs as listed on the Contract Data Requirements List (CDRL) by category of data, attached hereto, and made a part of this contract. Such data shall be prepared, maintained, and delivered to NASA in accordance with the requirements set forth within this document. In cases where data requirements are covered by a Federal Acquisition Regulation (FAR) or NASA FAR Supplement (NFS) clause or other term (e.g., requirements statement), that clause or term shall take precedence over the DRD.

Contract Data Requirements List (CDRL): Throughout the performance of the contract, the CDRL provides a listing by number, data type, title, and Office of Primary Responsibility (OPR).

Data Requirements Description (DRD): Each DRD included in this CDRL prescribes content, format, and submittal requirements. The DRDs included in this CDRL are ordered sequentially as listed in the CDRL page(s) that precede(s) the actual DRDs.

Data Type Description: Each DRD is classified by data type as defined below:

TYPE

DESCRIPTION

- 1 - All submittals of and interim changes to Type 1 DRDs require written approval from the contracting officer before formal release for use or implementation.
- 2 - NASA reserves a time-limited right to disapprove in writing any submittal of and interim changes to Type 2 DRDs. The contractor shall submit the required data to NASA for review within the time period established in the DRD prior to its release for use or implementation. The contractor shall clearly identify the release target date. If the data is unacceptable, the contracting officer will notify the contractor within the time period established in the DRD 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 the contracting officer within the time period established in the DRD.
- 3 – Type 3 DRDs shall be delivered as required by the contract and do not require NASA approval.

STATEMENT OF GENERAL REQUIREMENTS

Subcontractor Data Requirement

The prime contractor is responsible for flowing down any specific data requirements that apply to subcontracts and vendor agreements.

Reference to subcontractor data in the contractor's responses is permissible and a copy of the

referenced subcontractor data must be supplied with the response document at time of delivery to NASA.

Data Distribution, Format, and Transmittal

Distribution: Distribution recipients and number of copies are identified within each DRD and provided within the contract.

Format

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, or PowerPoint, as appropriate.

Hardcopy Format: Hardcopy of data deliverables is not required unless electronic delivery is not possible.

Transmittal: Data shall be transmitted to NASA as specified in the DRD.

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.

Data Transmittal Package: Each data transmittal package shall include a transmittal memorandum that specifies the following:

1. Contract number
2. Data Requirements Description (DRD) number
3. DRD data type
4. Submission date 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

Document Identification: 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. All Type I documentation 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.

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.

Document Revisions

Revisions of documentation previously submitted may be accomplished either by individual page revision or by a complete reissue of the document.

A 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.

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

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

All revised pages shall be identified by a revision identifier 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 using vertical line in the margin of the page, and the change authority shall be indicated adjacent to the change.

ALTERNATE CONTRACTUAL DATA PROCEDURES

NASA will provide an alternate on-line process to simplify and automate the submission of all required forms and information described in this document in place of the referenced e-mail submission process. The on-line applications and instructions for their use will be provided on the Contract Holder Only Page website prior to the date of submission requirements.

CDRL/DRD MAINTENANCE PROCEDURES

NASA-Initiated Change: New and/or revised data requirements shall be incorporated by contract modification to which the new or revised portion 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 is appended.

CDRL or DRD Change Procedures

Revisions to the CDRL or DRDs will be identified by NASA in the Document Change Log. The date of the revision, DRD number, title, and revision description will be annotated in the Document Change Log. Revision descriptions will include the modification number, which implements the change, and a brief description of the portions of the CDRL and/or DRD affected within the "Revision" column of the Document Change Log.

SEWP VI Contract Data Requirements List

DRD No.	DRD Type	DRD Title	OPR
2	3	AbilityOne Reporting	OP
3	3	Cybersecurity-Supply Chain Risk Management (C-SCRM) Plan	OP
4	3	C-SCRM Incident Reporting	OP
5		Climate Change Risk Management Plan	OP

1. DRD Title: AbilityOne Data Reporting		
2. DRD No.: 2	3. Data Type: 3	4. OPR: OP
5. Solicitation No.: TBA		6. Contract No.: SEWP VI GWAC
7. Date Issued: March 2024	8. Date Revised: N/A	9. DRD Category: Technical <input type="checkbox"/> Administrative <input checked="" type="checkbox"/> S&MA <input type="checkbox"/>
10. Description/Use: All Contractors competing and awarded a SEWP contract under NAICS Codes provided in A.1.34 NAICS and In-Scope NAICS Codes have a mandatory requirement to utilize AbilityOne non-profit organizations as Subcontractors on orders utilizing any of the referenced NAICS codes identified with an asterisk. All Contractors competing and awarded a SEWP order using Product Service Codes (PSC): D321 – IT and Telecom-Help Desk, DE01 – IT and Telecom – End User: Help Desk; Tier1-2, Workspace, Print, Productivity Tools (Labor), DE10 – IT and Telecom – End User As A Service: Help Desk; Tier 1-2, Workspace, Print, Productivity Tools, 7E20 – IT and Telecom – End User: Help Desk; Tier 1-2, Workspace, Print, Productivity Tool (HW/Perpetual SW), have a mandatory requirement to utilize AbilityOne non-profit organizations as Subcontractors utilizing any of the referenced Product Service Codes		
11. Distribution: SEWP Contracting Officers: gsfc-dl-sewp-space@mail.nasa.gov AbilityOne Program: www.abilityone.gov Initial Submission: October 1 st Submission Frequency: Every 12 months Format: Excel document per AbilityOne organization outlining each associated order Interrelationship: Article A.1.35 Applicable Documents: N/A Scope: This is required to account for the subcontracting amount associated with awards subcontracted to Ability One organizations. Contents: The contractor shall provide written notification to the SEWP Contracting Officer and the AbilityOne Program identifying the percentage of the total dollar obligated under AbilityOne. The notification shall identify best efforts made towards achieving the AbilityOne requirement and, if applicable, any rationale for failure to meet the requirement. Remarks: Emails should reference the header: [SEWP CH Name] AbilityOne Data Reporting: [Name of AbilityOne Organization]. The excel spreadsheet can reference difference NAICS Codes and PSCs. Maintenance: N/A		

1. DRD Title: SEWP Cybersecurity-Supply Chain Risk Management (C-SCRM) Plan DRD		
2. DRD No.: 3	3. Data Type: 3	4. OPR: OP
5. Solicitation No.: 80TECH24R0001		6. Contract No.: SEWP VI
7. Date Issued: APRIL 2024	8. Date Revised: N/A	9. DRD Category: Technical <input type="checkbox"/> Administrative <input checked="" type="checkbox"/> S&MA <input type="checkbox"/>
10. Description/Use: Contractors needs to provide a Cybersecurity Supply Chain Risk Management (C-SCRM) plan accounting for threats and impacts to cybersecurity supply chain risk. A C-SCRM incident is any disruption to the supplier of, or SDLC of a covered article that could include, but, are not limited to: <ol style="list-style-type: none"> 1. Malware or ransomware attacks targeting a supplier's systems, leading to the compromise of sensitive data or disruption of operations. 2. Insider threats within a supplier organization that results in the theft or manipulation of data. 3. Third-party software vulnerabilities that are exploited by threats actors to gain unauthorized access to the supply chain network. 4. Counterfeit components or products being introduced into the supply chain, leading to quality issues or security vulnerabilities. 5. Lack of proper security controls or standards within a supplier's infrastructure, making them more susceptible to cyberattacks. 		
11. Distribution: A C-SCRM Plan must be submitted to the SEWP Program Management Office and will be incorporated into the contract as Attachment J. Initial Submission: The plan shall be submitted no later than 60 calendar days after contract award date. Submission Frequency: Updated annually. Format: The contractor's format is acceptable. Interrelationship: Article A.1.30.1 Applicable Documents: NIST SP 800-161(most current version) for additional guidance; Executive Order (EO) 14028 Scope: Contractor shall demonstrate that C-SCRM practices based on NIST standards and guidance are being utilized. Contents: An annual report noting certification with the current ISO 20243 standard including a copy of a valid active Open Trusted Technology Provider™ Standard (O-TTPS) Certification. Remarks: To learn more about O-TTPS Self-Assessed Certification and the O-TTPS Third-Party Assessed Certification, please view The Open Group's O-TTPS Certification Program page. For more information about the ISO 20243 Standard, view parts 1 and 2 on their website: <ul style="list-style-type: none"> • ISO/IEC 20243-1:2018 - Part 1: Requirements and recommendations • ISO/IEC 20243-2:2018 - Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018 Maintenance: N/A		

1. DRD Title: SEWP C-SCRM Incident Reporting DRD		
2. DRD No.: 4	3. Data Type: 3	4. OPR: OCIO
5. Solicitation No.: 80TECH24R0001		6. Contract No.: SEWP VI GWAC
7. Date Issued: APRIL 2024	8. Date Revised: n/a	9. DRD Category: Technical <input type="checkbox"/> Administrative <input checked="" type="checkbox"/> S&MA <input type="checkbox"/>
10. Description/Use: The Contractor is required to report any C-SCRM security incident(s) that involves a potential compromise for any Contract related system or data. The Contractor is also responsible for reporting C-SCRM incidents to agency customers impacted by the potential compromise by notifying the cognizant ordering contracting officer at the task order level.		
11. Distribution: The C-SCRM Incident Report shall be sent to the Contracting Officer via email to gsfc-dl-sewp-pmo-cs@mail.nasa.gov with the contract number, company name, and C-SCRM Incident Report in the email subject header.		
Initial Submission: Within 72 Hours of known incident.		
Submission Frequency: Corrective action plans will be submitted within 30 days of incident.		
Format: Contractor format is acceptable.		
Interrelationship: A.1.1 GSFC 52.211-90 Deliverable Requirements (Apr 2023)		
Applicable Documents: A.1.30.2. C-SCRM Incident Reporting		
Scope: This requirement is intended to assess a potential contractor's SCRM maturity. An 'incident' or 'information security incident' is a violation or imminent threat of violation of information security or privacy policies, acceptable use policies, or standard security practices.		
Contents: <p>The report must include the following:</p> <ul style="list-style-type: none"> • A detailed description of the incident • The date and time of the incident • The location • The affected system(s) and/or cybersecurity supply chain element(s), • Contract number any other related information involving the incident. 		
Remarks: N/A		
Maintenance: The contractor is required to provide a corrective action plan within 30 days of the incident to include the implementation of risk remediation and a risk mitigation plan.		

1. DRD Title: Climate Change Risk Management		
2. DRD No.: 5	3. Data Type: 3	4. OPR: OP
5. Solicitation No.: TBA		6. Contract No.: SEWP VI GWAC
7. Date Issued: April 2024	8. Date Revised: N/A	9. DRD Category: Technical <input type="checkbox"/> Administrative <input type="checkbox"/> S&MA <input checked="" type="checkbox"/>
10. Description/Use: The Climate Change Risk Management Plan shall identify climate-related risks that could negatively impact performance of any resultant task order(s). The plan shall include an overview of actions taken, or opportunities identified, to adapt to the climate-related risks that may have a substantive financial or strategic impact.		
11. Distribution: SEWP Contracting Officers: gsfc-dl-sewp-space@mail.nasa.gov Initial Submission: The Climate Change Risk Management Plan shall be submitted within 12 months of Contract Award. Submission Frequency: Annually at Contract Anniversary Format: The contractor's format is acceptable. Interrelationship: GSFC 52.211-90 DELIVERABLE REQUIREMENTS (APR 2023) Applicable Documents: N/A Scope: Climate Change Risk Management Plan is essential for proactively addressing the challenges posed by climate change, safeguarding assets, products, services, and adapting to the climate-related risks that may have a substantive financial or strategic impact. Contents: At a minimum, the Climate Change Risk Management Plan must address the following: <ol style="list-style-type: none"> 1. What is your process for identifying, assessing, and responding to climate-related risks for successful performance or delivery (e.g., migration of smoke from wildfires, increases in precipitation-driven flooding, extreme heat events, and inundation due to sea level rise and storm surge)? 2. What inherent climate-related risks have you identified that may have a substantive financial or strategic impact on your business? Provide details of risks identified with the potential to have a substantive financial or strategic impact on your business. 3. What is your business continuity plan? 4. Describe your disaster contingency, continuity plans and response protocols for potential event-driven changes (e.g., hurricane, earthquake, flooding, wildfire and etc.) and chronic risks due to longer-term shifts in climate patterns (e.g., changes in precipitation, increased average temperature, and sea level rise). 5. Describe which assets, products, and services would most significantly disrupt operations if they experienced short term acute impacts (i.e. degraded service, loss of service, equipment failure, loss of asset or other unacceptable outcomes). 6. Describe which assets, products, and services would most significantly disrupt operations if they experienced gradual long-term cumulative impacts (degraded service, loss of service, equipment failure, loss of asset or other unacceptable outcomes). Remarks: N/A Maintenance: Changes shall be incorporated by complete reissue.		