	National Defence Défense Nationale		Back to the DID List

DATA ITEM DESCRIPTION - DESCRIPTION DE DONNÉES

1. TITLE – TITRE	**2. IDENTIFICATION NUMBER - NUMÉRO D'IDENTIFICATION**
SECURITY SCOPE DEFINITION	**DID 3.10.4**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

The purpose of the Security Scope Definition is to provide a description of assets including their attack surfaces and attack vectors for the Weapon System. The process includes defining the overall security perimeter and environment at both the platform (weapon support capability) and system level.
This document is used as an input for the Security Risk Assessment CDRL 3.10.5.

4. APPROVAL DATE DATE D'APPROBATION	**5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE PREMIERE RESPONSABILITÉ (BPR)**	**6. GIDEP APPLICABLE D'ÉCHANGE DE DONNÉES PERTINENT**
TBD	NWSO Technical Authority (TA)	N/A

7. APPLICATION / INTERRELATIONSHIP – APPLICATION / INTERDÉPENDANCE

CDRL 3.10.4 and SOW paragraph 3.10.1 refer.
This DID contains the format and content preparation instructions for the data generated under the Work tasks described in the NWS O&M SOW.

8. ORIGINATOR - AUTEUR	**9. APPLICABLE FORMS - FORMULES PERTINENTES**
NWSO TA	NIL

10. PREPARATION INSTRUCTIONS – INSTRUCTIONS SUR LA PRÉSENTATION DES DONNÉES

10.1 Source Document

10.1.1 NWS O&M SOW Section 3, paragraph 3.10.4
10.1.2 Risk-based Cyber Mission Assurance Process
10.1.3 NIST 800-160 v1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
10.1.4 NIST 800-160 v2 Developing Cyber Resilient Systems: A Systems Security Engineering Approach

10.2 Content and Format

10.2.1 The Security Scope Definition must be prepared and delivered in Contractor format.

10.2.2 The Security Scope Definition must be documented using the objectives specified in NIST 800-160 Volume 1 and expanded upon using the guidance and methods specified in NIST 800-160 Volume 2 for cybersecurity or alternative standards acceptable to Canada. As a minimum the following must be detailed using the guidelines:
a. Asset Identification;
b. Security Perimeter;
c. Security Environment and Trust; and
d. Management of Changes in the Security Environment.

10.2.3 In addition, the Security Scope Definition must document the following using the guidelines in RCMAP for cyber mission assurance or alternative standard acceptable to Canada:

a. Identification of the assets that require risk assessment. Assets can be described in a nested way, from facilities, to platforms, to systems and their components. As a minimum, two levels of assets are suggested at the platform and system level;
b. Description of the assets, including their attack surface and their security environment. The five classes of attack surface (Logical, Sensing and electromagnetic radiations, Personnel, Physical and Indirect) are accompanied with corresponding security measures. At the system-level, this should include description of its functions(s), hardware features (e.g. processors, chipsets and memory, security features such as physical tamper resistance, tamper/intrusion detection, zeroization, cryptoprocessor etc.) and software features including use cases, operating systems including configuration information (users, rights and privileges, modes, etc.), applications and services, databases and security measure, including technical (e.g. directory/file permissions) and operational (e.g. portable media policy) measures;
c. Trust assumptions of external entities and assets; and
d. Identification of attack vectors. The identification of attack vectors should include a description of: the asset involved, its interface, the interacting entities, the security measures of the interacting entities and the nature of the interaction (authorized or unauthorized).

10.2.4 Security categorization of the Security Scope Definition deliverable must be performed upon creation of the document, as the Security Scope Definition or certain portions could be Protected. Security labelling and marking, as well as handling, storage and transmission of the Security Scope Definition must be implemented in accordance with National Defence Security Orders and Directives. In addition to the Security Marking, which is placed in the header and footer of each page, a set of informative statements will be printed on the cover, or first page, of the document and in some cases also on the Verso Page (the back-side of the Title Page or Cover Page) as required.

10.2.5 The Contractor will be responsible for conducting change management as described below:
a. The System Security Scope Definition must include a change history summary section which contains the following:
i. A clear and unique version/revision identifier for each submission or resubmission of the Security Scope Definition;
ii. Clear identification of revisions or amendments within the document from its previous submission; and
iii. Rationale for the revisions and amendments.
b. All the above revisions/amendments must be clearly identified within the document by using suitable change tracking feature in the Office Management Software used to produce the document, e.g. "Track Changes" feature in Microsoft-Word®, side bars etc.

Page 2 of 2
December 2020