	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 RISK ASSESSMENT	**DID 3.10.5**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

The purpose of the Security Risk Assessment is to document the evaluation of cyber vulnerabilities, threat vectors, their likelihood and impacts. Security risk assessment activities include scope definition, preliminary security risk assessment and full/final security risk assessment. The Contractor must support independent security testing by an organization approved by Canada as part of vulnerability management activities.
This document covers the preliminary security risk and full/final security risk assessment. The scope definition is to be covered in the System Security Scope Definition CDRL 3.10.4.

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 3.10.5 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 3.10.5
10.1.2 Risk-based Cyber Mission Assurance Process

10.2 Content and Format

10.2.1 The Security Risk Assessment must be prepared and delivered in Contractor format.

10.2.2 The Security Risk Assessment must follow an iterative approach starting with a preliminary RA that describes threat scenarios in a high-level manner and completing with a full RA that details threat scenarios down to the implementation level (refined into series of Tactics, Techniques and Procedures (TTPs)). The preliminary risk assessment is concerned with vulnerabilities in the architecture and design or in the operational procedures, while the full risk assessment is to be completed with identifying vulnerabilities in the implementation as well as in the existing security measures.

10.2.3 The risk assessment is to be documented in a traceable, iterative manner in order that threats and vulnerabilities found can be traced back to threats and vulnerabilities and can be managed throughout the NWS' lifecycle. For instance, a risk assessment update may confirm that a vulnerability in the design identified during an earlier iteration of the risk assessment is actually exploitable. As a minimum the following must be detailed using the guidelines:
a. Threat Condition Identification and Evaluation;
b. Threat Scenarios Identification;

c. Security Measures Characterization; and
d. Level of Threat Evaluation.

10.2.4 In addition, the Risk Assessment must document the following using the guidelines in RCMAP for cyber mission assurance or alternative standard acceptable to Canada:
a. Vulnerabilities found in terms of their engineering level: requirement, architecture, design, implementation or configuration;
b. Threats, likelihoods, impacts, related risks and decisions. Associated vulnerabilities must be indicated along with related security measures at the requirement, architecture, design, implementation or configuration levels. The criteria and the evaluation method to determine the level of threat should be specified; and
c. Mitigation measures integrated into the functional SSRs and in a hierarchical way, i.e. system, architecture, design and implementation/configuration items.

10.2.5 The Risk Assessment document must include a vulnerability matrix. At a minimum, the vulnerability matrix must include the responsible(s), the related asset(s) name(s) or identification number(s), the related architecture or design item(s), as well as the applicable mitigations and the type of vulnerability in terms of attack surface (Personal, logical, physical, sensing, indirect (supply chain) to support decision-making. The vulnerability matrix's structure should normally follow the system architecture and design hierarchy. The vulnerability matrix should make use of vulnerabilities reports that have been released for existing products (e.g. Common Vulnerabilities and Exposures (CVE) as part of assessing vulnerabilities. As part of the risk assessment, the discovered vulnerabilities should be added to this vulnerability matrix.

10.2.6 Security categorization of the Security Risk Assessment deliverable must be performed upon creation of the document, as the Security Risk Assessment or certain portions could be Protected and/or Classified. Security labelling and marking, as well as handling, storage and transmission of the Security Risk Assessment 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. Sections of the document that are classified may identify the classification level of each numbered item (i.e. headings, paragraphs) by placing (U), (C), (S) or (TS) before the text.

10.2.7 The Contractor will be responsible for conducting change management as described below:
a. The Security Risk Assessment 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 Risk Assrssment;
   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.