	National Defence Défense Nationale		Back to the DID List

DATA ITEM DESCRIPTION - DESCRIPTION DE DONNÉES

1. TITLE – TITRE	2. IDENTIFICATION NUMBER - NUMÉRO D'IDENTIFICATION
CYBER SECURITY FUNDAMENTALS PLAN	**DID 3.10.8**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

The purpose of the Cybersecurity Fundamentals Plan is to demonstrate how the Contractor will implement the Canadian Cyber Incident Response Centre's (CCIRC's) top 4 strategies to mitigate targeted cyber intrusions.

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 3.10.8 and SOW paragraph 3.10.8 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 3.10.8
10.1.2 Top 4 Strategies to Mitigate Targeted Cyber Intrusions, Canadian Cyber Incident Response Centre, May 2019

10.2 Content and Format

10.2.1 The Cybersecurity Fundamentals Plan must be prepared and delivered in Contractor format.

10.2.2 The Contractor must establish and implement a written Cybersecurity Fundamentals Plan for the NWSO that must document at a minimum, the following:

a. An application whitelisting plan describing how the system will prevent malicious software and unapproved programs from running;
b. A description of the patch management process to ensure software applications and operating systems remain free of known vulnerabilities. At a minimum, known vulnerabilities are those listed in the MITRE Common Vulnerabilities and Exposure (CVE) database;
c. An operating system lifecycle management plan to describing how operating systems will:
   i. Remain OEM-supported for security patches at all times during the system lifecycle; and
   ii. Remain upgradeable as modern operating system security technology progresses.
d. A plan to restrict administrative privileges within software applications and operating systems based on user duties; and
e. A listing of assets where any items a) through d) will not be present. For each item:
   i. Explain why the security control will not be present; and
   ii. Present a plan to manage the residual risk.

10.2.3 Security categorization of the Cybersecurity Fundamentals Plan deliverable must be performed upon creation of the document, as the Cybersecurity Fundamentals Plan or certain portions could be Protected and/or Classified. Security

labelling and marking, as well as handling, storage and transmission of the Cybersecurity Fundamentals Plan 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.

10.2.4 The Contractor will be responsible for conducting change management as described below:

a. The Cybersecurity Fundamentals Plan 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 Cybersecurity Fundamentals Plan;
   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