	National Defence Défense Nationale		Back to the DID List

DATA ITEM DESCRIPTION - DESCRIPTION DE DONNÉES

1. TITLE – TITRE	2. IDENTIFICATION NUMBER - NUMÉRO D'IDENTIFICATION
CONTINUOUS MONITORING PLAN	**DID 3.10.9**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

The purpose of the Continuous Monitoring Plan is to detail the detection and analysis processes, procedures and tools for continuous monitoring. Continuous monitoring activities range from real-time monitoring (e.g. intrusion detection, automated log analysis) to longer-term monitoring (e.g. vulnerability assessment and risk assessment, security audit, etc.), that is normally conducted offline.
Preparation for containment, eradication and recovery, as well as post-incident activity is to be covered in the Incident Response Plan CDRL 3.10.10.

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 3.10.9 and SOW paragraph 3.10.9 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 3.10.9
10.1.2 Risk-based Cyber Mission Assurance Process
10.1.3 U.S. National Institute of Standards (NIST) SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (doi: SP 800-137)

10.2 Content and Format

10.2.1 The Continuous Monitoring Plan must be prepared and delivered in Contractor format.

10.2.2 The Contractor must establish and implement a Continuous Monitoring Plan to the NWSO.The Plan must document at a minimum, the following:

a. Mission criticality statements to be monitored in the continuous security monitoring strategy;
b. The circumstances, e.g. before or after military operations, triggered by threat intelligence or anomaly detection, and frequencies, e.g. yearly, for monitoring and for ongoing assessment of security, must be established;
c. The monitoring activities to be conducted must be established and associated with the circumstances or frequencies. This includes real-time (e.g. intrusion detection, automated log analysis) and offline activities (e.g. vulnerability assessment and risk assessment, security audit, etc.);
d. A plan that includes the resources, tools, conditions (circumstances and frequencies), monitored cybersecurity events, and documentation necessary for each required monitoring activity must be established;

e. When identified or detected, the security events are to be analysed, categorized (incidents, vulnerabilities, threats, or events without adverse effects), reported and documented:
   i. Incidents should be passed on to incident response;
   ii. Threats and vulnerabilities without patches available must have their risks assessed;
   iii. The vulnerability matrix and threat reports must be updated;
   iv. Mitigation strategies must be proposed for the identified risks; and
   v. Risk decisions (accept, avoid, transfer or mitigate) must be taken.

f. Continuous risk assessment is to be conducted as part of continuous monitoring, including:
   i. Determination, planning, and conducting of cyber test activities;
   ii. Update of the mission criticality statements, when necessary and whenever mission dependencies change and/or new systems are added;
   iii. Update of the description of the assets;
   iv. Update of the identification of attack vectors;
   v. Update of the threats and vulnerabilities;
   vi. Update of the risks;
   vii. Proposition of mitigating measures;
   viii. Analysis of risks and decisions; and
   ix. Update of security documents.

10.2.3 A cross reference matrix must be provided within this document that shows the items listed above are covered within this document or other referenced documents.

10.2.4 Security categorization of the Continuous Monitoring Plan deliverable must be performed upon creation of the document, as the Continuous Monitoring Plan or certain portions could be Protected. Security labelling and marking, as well as handling, storage and transmission of the Continuous Monitoring 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.

10.2.5 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