	National Defence Défense Nationale		Back to the DID List

DATA ITEM DESCRIPTION - DESCRIPTION DE DONNÉES

1. TITLE – TITRE	2. IDENTIFICATION NUMBER - NUMÉRO D'IDENTIFICATION
SYSTEM SECURITY MANAGEMENT PLAN	**DID 3.10.2**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

The purpose of the System Security Management Plan is to outline and define the Contractor System Security Management Program which will be used to ensure protection of the system from cybersecurity threats both during system development and for in-service (operation and maintenance, repair and overhaul). The plan is to identify the scope and content of the security activities that are applicable at the weapon system, aircraft and system level, and include the means for demonstrating compliance with airworthiness requirements related to security concerns and cyber mission assurance.

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 3.10.2 and SOW paragraph 3.10.2 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 3.10.2
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
10.1.5 U.S. National Institute of Standards (NIST) SP 800-37 Rev.2, Risk Management Framework for Information Systems and Organizations

10.2 Content and Format

10.2.1 The System Security Management Plan must be prepared in the Contractor‘s format.

10.2.2 The System Security Management Plan must document the following:

a. Applicable Documents: A list of documents which apply as directives or guidance during the execution of the System Security Management Plan. The list must include pertinent legal, regulatory and other published Contract requirements applicable to the system under development. System security requirements and objectives are drawn from these documents;
b. Purpose: Statement of the objectives for system security engineering and of the principles which will be applied;
c. Organization: Describes the organizational placement and manning of the Contractor's security engineering management organization. Charts and diagrams may be used to show organizational and functional relationships;

d. System Security Engineering Management Program: Description of the planned activities to satisfy system security engineering program objectives. Use of charts or diagrams is encouraged to illustrate the program's functional interfaces, engineering and design requirements, activity milestones, management process and levels of effort for each program phase;

e. Program Data Flow: Illustration of the manner in which basic program data flows, indicating how the system security engineering organization will monitor all program efforts and make inputs to decision process; demonstrate that the System Security Engineering and Systems Engineering processes are fully integrated to ensure interdependencies are established and managed.

f. Consideration for classification of Cybersecurity Work: Description of the methodology used to ensure that only appropriately cleared personnel, as per the Security Requirements Checklist of this Contract, will Work on Cybersecurity. Note that the requirement for appropriately cleared personnel includes those conducting the cybersecurity tests, writing reports, as well as Contractual or administrative staff who process the delivery of the tests and reports. A description of the means used to safeguard any classified information resulting from cybersecurity Work. Classification of cybersecurity CDRLs and data aggregation security must be addressed.

g. System Security Engineering Functions: Description of the principal functions and specific tasks to be performed as required by the Statement of Work, including the following:

   i. Description of how security regulations and other program guidance will be identified and synthesized into a set of security requirements and objectives;

   ii. Integration of Security Functions with the System Engineering Process: Description of the process by which security inputs will be applied to system functional design, requirements allocation, trade—off study, and communications, electronic, and interface (CEI) design specification processes;

   iii. Security System Synthesis and Evaluation: Description of the method by which security system hardware, software, facilities and procedures will be synthesized and evaluated. This includes cybersecurity testing used to validate cyber mission assurance as described in CS-007 for Continuous Monitoring.

   iv. Configuration Control: Description of the manner in which system security engineering efforts will be integrated with system configuration control activities. An explanation of how the proposed changes to the system will affect security efforts must be included;

   v. Relationships with other Contractors. Outline of the methods by which system security engineering efforts of associate system Contractors, subcontractors, and vendors will be integrated within the overall System Security Engineering Program;

   vi. System Installation: Description of how the System Security Engineering and Industrial and Product Security efforts will be coordinated to ensure no security vulnerability is created during system installation;

   vii. Product Security: Description of how the major system components/products will be secured at the Contractor's assembly plants. Identification of the security manpower, facilities, equipment, and procedures to be used. The security interface with associate Contractors, subcontractors, and vendors must be included;

   viii. Documentation of the COTS/Supply Chain Dossier, identifying for all COTS items:
      1. Plans for managing security of COTS items;
      2. Source of the COTS item;
      3. Delivery and updating procedures;
      4. Selection justification; and
      5. COTS/Supply Chain security reviews.

   ix. Documentation of the security assurance process, including:
      1. Description of the methods to be used to conduct the MCAAV and Security Scope Definition;
      2. Plan for performing the Security Risk Assessment;
      3. Plan for defining security function specification, design and implementation including developing the Cybersecurity Fundamentals Plan;
      4. Plan for identifying security test requirements, test methods and criteria;
      5. Description of the methods used to produce the Security Requirements Traceability Matrix and Plan of Actions and Milestones; and
      6. Plan for developing the Continuous Monitoring Plan and Incident Response Plan.

   x. Provision of additional considerations for any legal or regulatory constraints regarding security functions (e.g., encryption), TEMPEST (including NONSTOP and HIJACK as applicable), RED/BLACK Engineering, and vulnerability discovery; and

   xi. Provision of additional Security considerations required upon transition to In-Service Support.

h. Continuing System Security Processes: Description of the manner in which the system security program, its functions and deliverables produced will be managed and updated post-acceptance and throughout the lifecycle of the weapon system.

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

10.2.4 The System Security Management Plan includes a life cycle management program for software applications and operating systems to ensure that they remain supported and free of known vulnerabilities. Known vulnerabilities are those listed in the MITRE Common Vulnerabilities and Exposure (CVE) database.

10.2.5 The System Security Management Plan includes: an Access Authority and Data Security Plan which at a minimum includes the following access control and data security measures:

a. Restrict physical access to servers;
b. Restrict administrative rights to the Operating System (O/S) to a minimum of personnel;
c. Establish password policy and control;
d. Maintain an access control list to protect each object including but not limited to menus, files and tables;
e. Assign and control object and system privileges by user;
f. Control new account creation;
g. Enable software auditing to record logins and user transactions on critical objects;
h. Maintain virus detection and protection capability;
i. Detect and isolate unauthorized system users, either from external threats or internal sabotage;
j. Prevent the running of malicious software and unapproved programs; and
k. Validate on a routine basis (at least once a month) that each system is patched current, in a secure configuration, and know vulnerabilities are mitigated.

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

a. The System Security Management 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 System Security Management 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 3 of 3
December 2020