Pièce jointe 3 – Questions et réponses

(English text will follow)

Nœud pas être vulnérable : Enclaver la cybersécurité sur les navires canadiens (W7714-207317/004/A)

Le présent document comprend des questions et des réponses liées au défi.

Avis de non-responsabilité : En cas de divergence entre le contenu du présent document et le document de la demande de propositions de l'AP sur le site Web Achatsetventes.gc.ca, un précédent juridique est accordé aux renseignements figurant sur le site Web https://achatsetventes.gc.ca/

No.	Question	Réponse
1	Le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) recherchent-ils une solution complémentaire (aux services des fournisseurs actuels) ou des outils et des applications élaborés sur mesure?	Les FAC recherchent des idées innovantes dans la portée définie. Un outil sur mesure, une solution exploitant les services d'un fournisseur ou un agencement des deux, s'il permettait d'obtenir les fonctionnalités décrites dans l'EDT, constitueraient des options acceptables.
2	Peut-on voir les dessins des systèmes de TO et de TPF du MDN/des FAC?	Les biens fournis par le gouvernement, y compris les dessins de réseau des systèmes de bord, ne seront pas communiqués.
3	Quel est le modèle de sécurité actuel?	Cette question est trop générale et il n'est pas possible d'y répondre.
4	Le MDN et les FAC ont-ils un modèle de réseau Purdue?	Cela dépendra du système. Certains systèmes sont des réseaux autonomes et d'autres le sont moins. Les détails sur les connexions, si elles existent, entre ces systèmes et les solutions d'entreprise varient d'un système à l'autre.

5	Comment les systèmes de TO et de TPF du MDN/des FAC communiquent-ils avec leur propre réseau informatique d'entreprise?	Les systèmes connectés aux solutions d'entreprise, ainsi que les structures des connexions, peuvent varier selon la solution fournie.
6	Quels sont les fournisseurs actuels du MDN et des FAC pour les systèmes de TO et de TPF?	De multiples fournisseurs et sous-traitants fournissent actuellement des solutions.
7	Peut-on en savoir plus sur les vulnérabilités classifiées? Le MDN et les FAC les communiqueront-ils?	Pour le moment, il n'est pas nécessaire de connaître les vulnérabilités classifiées pour répondre à la demande liée au défi. La conception devrait permettre d'appliquer des intrants de sources multiples, dans l'optique de pouvoir répondre à des besoins futurs.
8	Quels sont les types de protocoles sous-jacents utilisés par le MDN et les FAC (OPC UA, Modbus TCP/IP)?	On retrouve différents protocoles dans divers systèmes, y compris des protocoles exclusifs.
9	Le défi indique que la Marine souhaite obtenir des recherches, des outils et des technologies portant, par exemple, sur quatre domaines (découverte de réseaux, évaluation des vulnérabilités, appui à la prise de décisions et surveillance des systèmes). Les propositions doivent-elles aborder tous les résultats souhaités?	Les solutions proposées peuvent répondre à un ou plusieurs résultats visés dans la description du défi.

Attachment 3 – Questions and Answers

Knot vulnerable - Locking Down Cybersecurity on Naval Vessels (W7714-207317/004/A)

This document includes questions and answers related to this Challenge.

Disclaimer: Should there be a discrepancy between the content on this page and the CFP Solicitation documents on Buy and Sell, legal precedent is given to information on buyandsell.gc.ca.

No.	Question	Answer
1	Are DND/CAF seeking a bolt on solution (using existing vendors in marketplace) or custom tools and applications that are built specifically for DND/CAF?	CAF is looking for innovative ideas within this space. A custom tool, vendor solution or mixture of the two are all acceptable options if they are able to perform the functions described in the SOW.
2	Are network drawings of DND/CAF OT and PT systems available to view?	Government furnished property, including Network drawings of shipboard systems, will not be made available.
3	What is the current security model?	This question is too broad in nature and it is not possible to provide a response.
4	Does DND/CAF have a Purdue Network Model?	This will be dependent on the system. Some systems are stand-alone networks and some are not. The details on how these systems are connected (if at all) to enterprise solutions are specific to each system.
5	How do DND/CAF OT and PT systems currently communicate with their own enterprise IT network?	For systems that connect to enterprise solutions, the way in which the system is connected may vary depending upon the solution provided.
6	Which different vendors are DND/CAF using for their OT/PT systems?	There are many different vendors / sub-contractors that provide solutions.

7	Can more information be provided regarding to classified vulnerabilities? Will DND/CAF be providing these classified vulnerabilities?	Information regarding classified vulnerabilities is not required to address the Challenge requirement at this stage. The design should allow for inputs from multiple sources, in order to allow for future requirements.
8	What type of underlying protocols are DND/CAF using (OPC UA, Modbus TCP/IP)?	There are a number of different protocols across various systems, including propriety protocols.
9	The Challenge indicates that the Navy is seeking research/tools/technologies addressing but not limited to four areas (Network Discovery, Vulnerability Assessment, Decision support, System Monitoring). Do proposals need to address all Desired Outcomes?	Proposed solutions can address any or all of the listed Desired Outcomes listed in the Challenge description.