Statement of Requirements
Cyber Security Collaborations – Expression of Interest

Introduction

1. BAE Systems Australia (BAE-A) provides some of the world's most advanced, technology-led defence, aerospace and security solutions.
2. BAE Systems Australia is Australia's most versatile defence and security company. BAE-A offers the Australian Defence Force (ADF) and its security customers total capability in vital areas such as through-life support, security, logistics and systems integration.
3. As part of its Australian Industry Capability (AIC) Plan for the Hunter Class Frigate Program (HCF), BAE-A wishes to assess current capabilities in cyber product testing in Australia. This will initially be conducted via a feasibility study.

Purpose

4. BAE-A is seeking expressions of interest from Australian-owned cyber security businesses to explore requirements and potential provision of cyber services to Hunter and its Supply Chain that meet the requirements set out in this document.
5. BAE-A has a strong preference for working with Supply Nation-verified Indigenous cyber security businesses as part of this study.
6. Non-Indigenous businesses with supply chain subject-matter expertise and an interest in engaging with an Indigenous business or workforce are also particularly encouraged to participate in the study in an advisory and supporting role.
7. It is intended that up to five (5) organisations shall downselected from the EOI activity. Selection of these participating organisations shall be made in mid 2020.
8. It is expected that the organisations taking part in this EOI will work collaboratively with BAE Systems supply chain companies to achieve agreed outcomes.
9. Each respondent to this EOI is expected to fully inform itself on current trends and issues associated with cyber security in defence supply chains and provide relevant and comprehensive information in its response.
10. Respondents may be invited to discuss their EOI as part of the evaluation.

Scope

11. The scope of work will include the development of an Australian capability for overseeing and enhancing supply chain security.

12. This EOI seeks information on companies':
    a. Organisational structure
    b. Overview of cyber security capabilities.
    c. Capacity to deliver cyber security activities from Adelaide, South Australia.
    d. Understanding of cyber security standards relative to the delivery of Australian Defence

security requirements, including but not limited to the Defence Protective Security Policy Framework, Information Security Manual, ISO 9001 and ISO 27001.

e. Reference customers from previous cyber security engagements

Outcomes

13. Further collaboration and business opportunities may be offered to participating organisations as a result of their participation in this EOI.

14. All participating businesses shall receive feedback on capability requirements and opportunities for development.

Location and security clearance requirements

15. All organizations participating in the EOI shall be located within Australia and be expected to attend meetings, workshops and other sessions at BAE-A premises in Adelaide, South Australia.

16. All proposed personnel working with BAE-A and in this program shall hold a BASELINE security clearance at a minimum and be capable of clearance upgrade to NV2.

BAE supervision and direction

17. BAE-A appoint project managers from within our cyber security teams to perform management and oversight of work delivered under a potential resultant contract.

18. These project managers shall:

    a. Provide a primary point of contact between BAE Systems and participating organisations.

    b. Provide necessary materials and/or facilities.

    c. Provide an avenue for escalation of queries/issues.

    d. Review and provide feedback on all inputs to the study.

19. BAE-A staff, or supply chain partners, may work alongside the successful organisations to deliver work.