CO-115475-UOMM

CP120 – WP0 – URGENT OBSOLESCENCE MANAGEMENT MITIGATION

SCHEDULE A WORK PACKAGE 0.11

EXTENDED WARRANTIES FOR RSA AND KEYSIGHT

NATO Communications and Information Agency
Agence OTAN d'information et de communication

BOOK II, SECTION IV

STATEMENT OF WORK

TABLE OF CONTENTS

SECTION 1 – INTRODUCTION

1.1 Background Information

1.1.1 NATO's current Cyber Defence posture is based upon the NATO Computer Incident Response Capability (NCIRC) – Full Operational Capability (FOC). The NCIRC FOC scope was defined in the Strategic Commands' Statement of Operational Requirement (SOR) (reference [NCIRC SOR]). NCIRC FOC is a Cyber Defence capability, deployed in a 'hub-and-spoke' architecture.

1.1.2 Tier-2 infrastructure is the pillar on which every service within NCIRC is based for network, security, servers, workstations, virtualization, storage, backup and monitoring requirements. It also supports the sum of all capacity and performance requirements of every NCIRC subsystem.

1.1.3 Tier-2 infrastructure includes the following:

1.1.3.1 Network Intrusion Detection/Prevention Systems (NIPS) provide NCIRC with the capability to identify potential cyber-attacks on NATO networks and to log information about this malicious activity. The sensors are managed by the Defence Centre Central Management Capability. The NIPS Tier-2 infrastructure has already been upgraded to the latest version and is therefore not included in the scope of this SOW.

1.1.3.2 Full Packet Capture System (FPC) provides to the NCIRC the capability to store locally on the protected Tier-3 sites a record of the network traffic at various critical points. The FPC Tier-2 infrastructure has already been upgraded to the latest version and is therefore not included in the scope of this SOW.

1.1.4 Tier-3 infrastructure includes the following:

1.1.4.1 Tier-3 Full Packet Capture System (FPC) provides to the NCIRC the capability to store locally on the protected Tier-3 sites a record of the network traffic at various critical points.

1.1.4.2 Tier-3 Enclave encompasses all infrastructure and hosting components necessary to instantiate the requisite Tier-3 sensors and subsystems, and to facilitate their interaction with Tier-2, and their central management. With the exception of CSO Paris, Tier-3 Enclaves have been deployed at all defined sites, on all available Security Domains - NATO Unclassified (NU), NATO Restricted (NR) and NATO Secret (NS).

1.2 Requirements Overview

1.2.1 This Statement of Work (SOW) describes requirements the NCI Agency is seeking in the procurement of extended warranties required for cyber security equipment which is being deployed to replace equipment and systems that have reached End of Life (EoL) or End of Support (EoS). This project is referred to as Urgent Obsolescence Management Mitigation (UOMM).

1.2.2 These systems are part of the existing NCIRC, which is operated centrally at Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium.

1.3 Contract scope

1.3.1 The Contractor shall provide extended warranties from 1 January 2023 until 31 December 2023 on equipment detailed in Annex A.

1.3.2 The RSA equipment will be located at the following sites:

- Mons – BEL
- Norfolk – USA
- Brunssum – NLD
- Geilenkirchen – DEU
- Ramstein – DEU
- Paris – FRA
- Brussels – BEL
- Aix en Provence – FRA
- Lago Patria – ITA
- Izmir – TUR
- The Hague – NLD
- Poggio Renatico – ITA
- La Spezia – ITA
- Torrejon – SPA
- Monsanto – POR
- Capellen – LUX
- Betzdorf – LUX
- Northwood – UK
- Uedem – DEU
- Munich – DEU
- Bydgoszcz – POL
- Stavanger – NOR

1.3.3 The Keysight equipment will be located at the following sites:

- Mons – BEL
- Paris – FRA
- Bettembourg – LUX
- Brunssum – NLD

1.3.4 The Equipment is split into two different technologies:

1.3.4.1 RSA equipment will require a warranty providing 24/7 support.

1.3.4.2 Keysight equipment will require an Essential Global Support Warranty.

1.4 Standards for interpretation of the SOW

1.4.1 Context information supporting the requirements definition are provided using the term "may". "Shall" statements are contractually binding; "May" statements are non-mandatory, or they imply intent on the part of the Purchaser.

Annex A

A.1 RSA Equipment is detailed in the following table:

Model Number	Component Type	Item Description	Quantity
NW-PVHDE96	FPC Decoder Storage Drive	RSA NETWITNESS PV HP 96TB SED (E03J)	92
NW-PVHPE78	FPC Concentrator Storage Drive	RSA NETWITNESS PV HP 78TB SED (E03J)	46
NW-S6E-CORE-NL	FPC CORE	RSA NETWITNESS S6 SED CORE TP APPL - NO SW LIC (E39S)	140
NW-S6E-HYBRID-NL	FPC-1	RSA NETWITNESS S6 SED HYBRID TP APPL - NO SW LIC (E38S)	14
NW-S6E-ANALYTIC-NL	FPC ANALYTIC	RSA NETWITNESS S6 SED ANALYTIC TP APPL - NO SW LIC (E39S)	2

A.2 Keysight Equipment is detailed in the following table:

Model Number	Component Type	Item Description	Quantity
SYS-E10S-16P-AC	Aggregator	IXIA ASSY, Vision E10S Base system, AC	9