Annex A – Summary of Requirements

Project No. 2020/0IS03301, CP9C0150

1. Project Objective

a) The Privileged Access Management (PAM) project is part of the wider IT Modernisation (ITM) Recovery Increment 1 project, aiming at providing the following services through the Operational Network (ON): Infrastructure as a Service (IaaS), Enterprise Core Services (ECS), Client Provisioning Services (CPS) and Service Management and Control (SMC).

b) The PAM project will deliver a comprehensive solution to control and audit privileged accesses, actions and permissions by elevated users managing the IT environment.

2. Scope of Work

a) The scope of the PAM service is all NCI Agency provided CIS, where privileged access accounts are needed to some extent.

b) The implementation of PAM, will follow the ITM implementation, with its respective spirals and increments.

c) The successful contractor will carry out an end-to-end project, from analysis and design to implementation, taking into account the current and future challenges and constraints of the NATO environment.

d) PAM-Professional services are required activities.

e) The project will follow a phased roll-out approach. Required PAM measures include:

- Inventory of privileged accounts
- Implementation of multi factor authentication of privileged accounts, using the NATO PKI-system.
- Establishing controls for privileged access
- Account/credentials vaulting
- Session management
- Session recording
- Rationalise number and scope of accounts and privileges
- Implementation of Just in Time access controls
- Integration with SIEM
- Integration with tooling like ITSM/IGA
- Automation of privileged tasks

- User based analytics

f) The PAM system is expected to integrate with all Communication and Information Systems, amongst which:

   i. Network equipment (e.g. routers, switches)

   ii. Security Enforcing Infrastructure (e.g. Firewalls, VPN-concentrators)

   iii. OSs (e.g. Linux, Windows, Solaris)

   iv. Applications (e.g. containerized, COTS, web-based, legacy)

   v. IoT/OT devices (e.g. Building Management, Cameras, Security Systems)

3. Geographical Implementation

a) The solution will be primarily implemented in NATO authorized NATO Command Locations in Europe in Brussels (Belgium) and Lago Patria (Italy). If required to support specific integrations, travel to other NATO Command Locations in Europe and North America, may be required. The NATO organization is detailed at: http://www.nato.int/cps/en/natolive/structure.htm.

4. Warranty and O&M Support

a) Following acceptance of the final operational delivery, the contract will require warranty for any software delivered.

b) The contract is expected to include O&M support following acceptance of the final operational delivery.