Annex A – Summary of the Requirements

1. Introduction

The Information Exchange Gateway Case C (IEG-C) project will provide:

- Support for Information Exchange Services of critical information and real time data between the NATO Secret core network (which comprise NATO commands, agencies, and connected NATO Nations) and Mission Secret networks (for NATO Responses Forces, NATO-led Coalition Exercises or Operations).
- These services will be provided by a gateway, which should be able to scale based in the needs of the supported mission, available bandwidth and response times.
- These gateways may be in deployed positions but will be centrally managed, monitored and controlled, while physical maintenance will be undertaken by local staff.
- The main objective of the gateway is to protect NATO Secret (NS) Network from unauthorized access from the NATO-led Mission Secret (MS) network, and to prevent the release of un-authorised data. The gateway will mediate exchange of data for both ‘core’ and ‘functional’ services.

2. Project Scope

This project will provide the system for securing information exchange services between the NATO Secret Bi-SC AIS and the NATO-led Mission Secret networks by the implementation of secure gateways, replacing the prototype gateways in current use, and conform to recently approved NATO Metadata STANAGs (4774, 4778). The project will provide a standardized architecture for IEG-C, resolving deficiencies and improving management capabilities by including a centralized management capability. The current gateways will be upgraded, redesigned or renewed to comply with this architecture.

The IEG-C services will be partly virtualised and hosted on the infrastructure provided by the Agency and procured through the ITM contract.

The aforementioned information exchange services shall include in particular:

- Text Chat
- Electronic mail
- Directory Services
- Web Services
- Common Operational Picture Data
- Video Teleconferencing
- Tactical Data Links data
- Secure Voice over IP

IEG-C will be robust and reliable, with a 24/7 availability.

IEG-C will utilise certificates provided by the NATO Public Key Infrastructure (NPKI) service.

The IEG-C project scope includes:

- Project management
- Requirements Analysis, System Engineering/Design, Testing, Site Surveys
- Security accreditation
- Site implementation
- Initial support

3. Geographical implementation

The IEG-C Service will be installed in 6 locations and managed centrally from SHAPE Mons, as follows:

Mandatory Sites

- SHAPE (Mons, Belgium)
  - NATO Response Force (NRF)
  - Very high-readiness Joint Task Force (VJTF)
  - Exercise
  - Reference System & Management Facility
- JWC Stavanger
  - Exercise 1
  - Exercise 2
- EUROCORPS Strasbourg
- Allied Rapid Response Corps (ARRC Innsworth)
- JFC NAPLES (Lago Patria, Italy)
  - Active Endeavour
  - NRF Standby
- Joint Force Training Centre (JFTC) Bydgoszcz
  - Exercise 1

Optional Sites

- NCIA Testbed (The Hague, The Netherlands)
- HQ Kabul (Resolute Support)
- KFOR Pristina

- EUFOR Sarajevo
- JFC NAPLES (Lago Patria, Italy)
  - Ocean Shield
  - Resolute Support
- Afloat Command Platform (NATO flag ship)