a) CP5A0050 Core Services and CP5A004 Military Message Handling System – These two CPs provide the core services to the Alliance AIS and will be combined into one single CP titled CP9C0150 Core AIS for Static Commands. Implementation is based on evolutionary acquisition and spiral development that is to be executed over the next five to ten years. **A large majority of MGSC’s opportunities will come out of this CP.**

b) CP0A0149 Deployable CIS – Provides a readily deployable and trained CIS capability to the NATO Combined Joint Task Force and NATO Response Force. While a portion of this CP supports the Alliance AIS, it is much broader and will be addressed separately in this section as one of the four major programs.

c) CP0A1303 Active Layered Theater Ballistic Missile Defense – This CP provides an Alliance-wide capability to protect deployed forces from tactical ballistic missiles. It is based on an incremental approach and will consist of collaborative tools for planning, force generation and intelligence preparation, a real-time battle management function, a communications capability interfacing with the Alliance AIS and riding on the NGCS, and a system of systems required to interface and exchange information. **The first increment of this program has already been awarded to SAIC.**

d) CP0A0109 Air Command and Control System – Provides a real-time command and control system for air operations. **Very few if any of this CP’s projects will result in opportunities for MGSC.**

e) CP5A0007 Operations Functional Service (FS) (Joint, Air, Land) and CP9B3013 Maritime Operations Command and Control Information System – Provides a command and control information system for joint, air, and land in the first CP and maritime in the second CP. The initial project that will provide an opportunity for MGSC is the NATO Common Operating Picture. Eventually the two CPs will be combined into one – CP9C0107 Ops Functional Services. Implementation is based on evolutionary acquisition and spiral development that is to be executed over the next five to ten years. **The value of this CP at the time of publication of this document was unknown but is expected to be substantial and one in which MGSC will be interested in pursuing.**

f) CP0A0110 INTEL Functional Services (FS) – Provides all NATO HQs with information system services supporting the specific business of the intelligence support. It initially integrates existing legacy intelligence systems into an integrated functional service. Implementation is based on evolutionary acquisition and spiral development that is to be executed over the next five years. The INTEL FS spiral 1 is expected to be released for bid in 2008 with the follow-on spiral expected two years later. **This CP is valued at over 20M€ with a potential additional 22M€ following a CP amendment covering 2 additional increments.**

g) CP9C0103 Logistics Functional Services – Provides all NATO HQs with information system services supporting the logistics functions. Little information was available on this CP at the time this document was written because approval of the CP has been delayed.

h) CP5A0053/9B0010: Personnel Functional Services – Provides information systems services for personnel management. **The projects in this CP have been competed and already awarded.**

* + 1. NATO General Purpose Communications System (NGCS) Program

The NATO General Purpose Communications System (NGCS) provides the fixed static network or core communication services in support of Alliance Command & Control, Consultation (C3) and the Non-C3 requirements associated with Partner Coalition and Exercise. The NGCS uses CP0A0104 – Alliance Core Communications Services to expand on the existing NATO wide-area network. Add maritime and why we’re not doing maritime.

**The scope of the NGCS program encompasses 12 different projects in CP0A0104 valued at over 255M€.** It provides a baseline Target Architecture with a follow-on future Target Architecture, circuit switched components, packet transport components, network-network gateways, studio video teleconferencing, network and service management, extension to new member nations, public information access gateways, and a Program Management Office to exercise configuration management and life cycle support. The Target Architecture effort is incremental and the network services will be implemented incrementally while much of the expansion of the network and additions/improvements to the infrastructure will be released in separate projects. **MGSC is currently bidding on the first increment of the Target Architecture as a sub-contractor to British Telecom and will be well positioned to do the follow-on architecture work as well as other future network projects if successful in winning the Target Architecture bid.** Appendix E depicts the NGCS baseline in 2008 to the future NGCS in 2014.

* + 1. Cyber Defense and Information Assurance Program

Currently, NATO’s information assurance and cyber defense capability is in its infancy with an initial limited computer incidence response center, inadequate information security (INFOSEC) management, and antiquated encryption and electronic security equipment and key management system. CP0A0155 Electronic Information Security Services will bring NATO’s information assurance and cyber defense capabilities into the 21st century. Because of restrictions imposed by the ITAR on the sale of encryption/cryptographic equipment and key management systems to foreign governments, this portion of CP0A0155 will not be viable to MGSC. However, the remaining scope of this program provides opportunities to MGSC and encompasses a more complete and robust NATO computer incidence response center with an intrusion detection system, secure information exchange interfaces to protect gateways, and a system and tools for effective INFOSEC management and support. **The scope of the Cyber Security and Information Assurance program applicable to MGSC encompasses 5 different projects in CP0A0155 valued around 14M€.** While this represents a much smaller total value as compared to the 3 other major programs addressed in this section, it fits very well within MGSC’s core competencies and is given a relatively high ranking in NATO’s CP priority listing. As with any other institution, the threat of a major attack on NATO’s networks is very real and would have a significant impact on operations so one can expect to see continued if not increased funding for NATO’s limited information assurance program.

* + 1. NATO Deployable Communication and Information Systems (DCIS) Program

The NATO Deployable CIS (DCIS) Program provides a deployable communications and information system to NATO’s Combined Joint Task Force (CJTF) and most recently to their NATO Response Force (NRF) and is one of NATO’s top priority programs. A portion of the scope of the DCIS does not fit within MGSC’s core competencies such as providing deployable SATCOM and non-SATCOM transmission equipment; UHF, SHF and EHF secure transportable ground terminals; deployable non-CIS equipment; and civil engineering work. However, a number of projects will and have already provides communications components for local area networks, information systems components, VTC equipment, information security components, and office equipment to configure the office module shelters for CJTF and NRF. CIS at garrison HQs is programmed in CP5A0050 – Bi-SC AIS Core Services. **The NRF portion of this CP is on a fast timeline and it is expected that NATO will release an NOI for NRF Deployable CIS in the near future.** This and other near term DCIS opportunities will need to be deconflicted with MSS. **The scope of the DCIS program applicable to MGSC encompasses 5 or 6 different projects valued at over 150M€ over the next 13 years. The total expenditure over the next five years is 88M€ with the bulk allocated to the NRF.**

* 1. Mapped to MGSC Core Competencies

The obvious next step in MGSC’s NATO acquisition strategy is to map potential NATO projects in CPs identified above to MGSC’s core competencies. The NATO Business Development lead is well underway to identifying opportunities for the next three years; however, CPs should be examined for future opportunities beyond 2009. And, the same needs to be accomplished for updated CPs and new CPs. **The MGSC Business Development lead should accomplish a review of CPs with the ManTech lead in Brussels for opportunities coming in the following year and for the next three years no later than July of each year.**

Projects in CPs should be examined to determine if they map to the following MGSC core competencies: 1) Cyber Security and Information Security; 2) Network Operational Security; 3) Certification and Accreditation Support; 3) Information Operations, Analysis and Computer Forensics; 4) Application Design and Development; 5) Signal Processing and Signal Intelligence analysis applications; 6) Enterprise Network Design, Integration, Maintenance, and Administration; 7) Enterprise Solutions specializing in information sharing using collaborative tools, enterprise application integration, and database technologies; and 8) IT Modernization in such areas as receiving, inventory management, warehouse storage, site surveys, integration and testing, and packing and shipping. **However, MGSC should not rule out projects where some requirements do not fall within MGSC’s core competencies because in most instances teaming agreements can be carefully negotiated with sub-contractors to perform work in which MGSC is not experienced.**