

# ICCRTS Remarks

C2 Policy Panel

# DoD's C2 systems are Evolving to Services Oriented Architecture Technology

- What is SOA?
- Why is DoD Adopting SOA?
- Does SOA Impact C2 Policy?
- What Should Be Done to Address the SOA Issues?

# What is SOA?

- Services Oriented Architecture is a Web Services based technology that is powering today's most capable e-businesses
  - IBM has transformed the company to run on SOA internally
- Widely adopted open standards enable inherent interoperable
  - SOA is about machines talking to machines to free up the human users
- SOA does not require a green field solution
  - Legacy applications can be wrapped into SOA standards to create interoperability and evolutionary growth
- SOA allows loosely coupled business applications to interoperate with little or no IT and software support
  - Distributed DoD or allied users can provide service and application elements for all to adopt and use
- SOA supports the dynamics of today's changing business or military missions
- SOA services and applications enable composeable functions to support real world changes
  - i.e. mixing new sensor information into a mission workflow could be done in weeks rather than years as has been our history

# Why is DoD Adopting SOA?

- Joint DoD is about interoperability and SOA technology promises better opportunity for success than in past technology/policy eras
- Currently DISA and each of the Military Services are working on some form of SOA upgrade to existing C2 systems
  - NCES (Net Centric Enterprise Services) will provide core SOA services
  - JC2 and Service Communities of Interest will provide mission capability

# Does SOA Impact C2 Policy?

- The GIG is an SOA enabled DoD mandate that has been policy enabled
  - GIG BE has provided the large pipes to enable needed bandwidth
  - NCS and soon JC2 are moving to build the future core C2 capability
- To date no policy has been created to require that SOA components will be reuseable and interoperable
  - Dynamic mission flexibility and composeable capability will not be achieved without the added rigor of SOA component certification

# What Should Be Done?

1. Establish policy that requires all SOA software, including adopted legacy applications, to be certified through active testing
2. Adopt existing DoD C2 governance bodies to set certifications standards and interoperability requirements
  - Based on government and industry expert bodies
  - Using widely adopted commercial open standards
3. Establish a hierarchy of certification centers
  - Operated at DoD, Service, Agency levels to ensure rapid response to new products
4. Secure certified service and application pieces to protect the products developments
  - PKI or equivalent certificates could be electronic gateways for operational system use
  - For the first time in DoD history, real control of system participation could be enforced

# What is the Cost of SOA Certification?

- SOA productivity and operational flexibility far exceed previous technology eras
- Certification centers could be funded by application builders similar to security hardware certification
- Reuse and interoperability will easily offset the cost of certification and use control infrastructure

# SOA C2 Policy Summary

1. SOA promises mission flexibility and system interoperability superior to previous technology generations
2. The promise cannot be achieved with today's policy
3. Policy that requires reuse and SOA component interoperability must be created
4. Validation certification and system level enforcement can ensure policy compliance