

12<sup>th</sup> ICCRTS  
“Adapting C2 to the 21<sup>st</sup> Century”  
“DOD COI Governance and Defense Contractors”  
Track(s): TBD  
Duane McCollum  
The Boeing Company  
P.O. Box 3707, MC 84-71  
Seattle, WA 98124-2207  
253-657-1707  
206-491-0794 (Cell)  
[duane.j.mccollum@boeing.com](mailto:duane.j.mccollum@boeing.com)

Title of Paper: “DOD COI Governance and Defense Contractors”

Author’s suggested tracks

Track 5: Organizational Issues

Classification: Unclassified

Abstract:

This paper builds on Scott Renner’s 2006 CCRTS submission, “My Two Cats Are a Community of Interest” by identifying information management governance issues for defense contracting companies who may have to participate in DOD COIs as a part of their work on acquisition programs. Currently, COI governance, membership make-up, and other details of participation generally depend on the COI itself. However, this loose structure challenges program managers of defense contracts as they must now determine how to adjust their organization to this new information sharing model. Information management governance generally addresses accountability, ownership, and disclosure. Contracting companies must carefully study the costs and benefits to participation to understand how to balance the implementation of the Net Centric Data Strategy to potential unintended consequences of program or corporate sensitive information getting into the wrong hands as a result of COI participation. The relationship dynamic between contractors and their government clients are challenged as contemporary program protection practices and policies may have to be changed. The stewardship of a company’s intellectual property, the function of firewalls to manage fair competition among partners and other issues exist. This paper presents categories of risk and suggests frameworks to follow for the near term.

Keywords: DOD Communities of Interest, Information Management, Net-Centric transformation governance.

Note: The following paper does not reflect the policies of The Boeing Company concerning DOD COIs.

## Summary

Currently, COI governance, membership make-up, and other details of participation generally depend on the COI itself. However, this loose structure challenges program managers of defense contracts as they must now determine how to adjust their organization to this new information sharing model. Information management governance generally addresses accountability, ownership, and disclosure. Contracting companies must carefully study the costs and benefits to participation to understand how to balance the implementation of the Net Centric Data Strategy to potential unintended consequences of program or corporate sensitive information getting into the wrong hands as a result of COI participation.

## The Problem

Bob arrived late to the *Joint Tactical Informatics* COI meeting. This was the COI's third meeting and Bob's first time to any COI meeting. His manager gave him minimal instructions other than 'just show up and see how we can influence the COI's work' in their program's favor. Once he arrived at the meeting, he was surprised to see the conference room filled to standing room only. There was one chair left open, and next to it sat a man whom he recognized. Although he remembered the guy's face, he could not remember the name. Being in an unfamiliar situation, any familiar face was welcome, so he gingerly crept past several people who were absorbed in a presentation given by a high-ranking service official in the front of the room. Bob managed to sit next to this fellow and learned his name was Ray. While the presentation continued, they started to chat in low, but polite, whispers:

"We're making great progress on forming a consolidated tactical thesaurus", Ray whispered. "We've got vocabularies from several existing programs already. I am leading the COI in building our pilot ontology for knowledge retrieval."

"OK, that's something I don't really get. How do you mean 'vocabularies'? My program, the Integrated Space Mission Command Systems, only has a DODAF AV-2 --is that what you mean by 'vocabulary'?", asked Bob.

"Oh, yeah, well, an AV-2 is not *really* what we're after. We really need taxonomies, ontologies, or even data models --anything that describes how a system manages and categorizes data".

"A Data model? Heck, I've got an older version from our program right here on my thumb drive. Can you take a look at it and see if it's what the COI needs"?

Although Bob was just trying to be helpful there may have been risks he was taking by sharing his program's data in just this way. Have such conversations occurred in COI meetings, especially during their forming and development phase? Perhaps they have, in one form or another. Even if they haven't, such a scenario should give pause to any acquisition Program Manager, especially those working for commercial companies. Add to this fictional scenario the idea that Ray and Bob are contractors: one, perhaps, employed by a large aerospace firm, the

prime on a new POR; the other a Federal agency. So, the sharing of information between them should probably not be so casual.

Scott Renner, in his 2006 ICCRTS paper “My Two Cats Are a Community of Interest”, defines DOD Communities of Interest as “a group of people who cooperate to solve a problem in net-centric data sharing”.<sup>1</sup> In solving their data sharing problems, they may have to create a common vocabulary (as in the fictional COI in the above scenario), useful for discovery metadata, data exchanges, and other purposes. The basic nature of a COI, it is assumed, is a collaborative group of people drawn from multiple organizations solving a data-sharing problem, which cannot be solved under their current information management structure. Renner observed there does not exist a common standard of information management governance applicable to all COIs. He also believed it is important to discuss roles and responsibilities of COI Information Management and governance in order to mature the COI concept and promote its potential efficiencies. Renner’s most important point was for us “to think less about COIs per se, (and) instead turning our attention to the COI members, and their roles and responsibilities”.

Implementing a governance structure on two cats may in fact be easier than one wholly applicable to DOD COIs. Nevertheless, Program Managers must be aware of the information management governance issues for defense contracting companies who may have to participate in DOD COIs as a part of their work on acquisition programs. As of this writing, the policies of COI governance, membership make-up, and other details of participation generally depend on the COI itself. Contracting companies must carefully study the risks and benefits to participation to understand how to balance the implementation of the Net Centric Data Strategy to potential unintended consequences of program or corporate sensitive information getting into the wrong hands as a result of COI participation. The relationship dynamic between contractors and their government customers may be challenged as contemporary program protection practices and policies may have to be changed. But to what extent? The stewardship of a private company’s intellectual property, the function of firewalls to manage fair competition among partners, and other issues still exist (regardless of the potential leap of data sharing innovation COIs may bring). This paper explores the potential governance issues facing participants in COI *developmental* activities.

## **Risks to a Commercial Company Participating in a COI**

Understanding the terminology used to describe a problem, or the solution to a problem, is very important. For instance, the term ‘governance’, as it is used in the corporate world seems to refer to an *accountability framework*. Governance then is usually about accountability, transparency, and disclosure. All of these activities are dependent on reliable information to be effective. For instance, the lack of reliable information lead to insufficient governance that accounts for some of the causes to the collapse of Enron. For a basic reference, the ITGI (Information Technology Governance Institute) defines IT Governance as follows:

“IT governance consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives”.<sup>2</sup>

The current use of the term ‘governance’ in the context of DOD Communities of Interest has a different cast. Here, COI governance refers less to an accountability framework and more toward an *expectations and management*, an IT portfolio framework and falls (more or less) under DODD 8115.01 (October 10, 2005) the “Information Technology Portfolio Management”.

A Program Manager should be aware of and should be able to classify the benefits and risks to their program by participating in COIs. In other words, there is a need to know how benefits and risks are identified and resources managed. In the corporate setting, good process management and governance *adds value* to the business mission. For COIs, good process management and governance should help the members (and their home organizations) adequately identify benefits and risks --while the COIs proceed on their mission.

A Program Manager should have oversight into COI participation. There should be a set of mutually understood expectations, terminology, goals, and processes. Some of the process questions a PM may consider are the following:

1. Identify all members of the COI. Know who they are, what companies or components they work for.
  - a. If there are potential conflict of interest issues, raise them to the appropriate channel. Carefully document all concerns and see to it they are addressed.
  - b. Consider the potential may exist of inadvertently exposing intellectual property to a competitor.
2. Request a COI charter; if there is no charter, request that one be drafted by the COI leadership; if none is to be forthcoming, consider not participating.
3. Identify any of your company’s intellectual property that might be shared with or potentially used by a COI, and perform a risk analysis on the costs and benefits.
4. Understand the rights of ownership in creating any work products such as taxonomies, ontologies, vocabularies --or even things like simple scripts to automate MS applications.
5. Continually collect and provide analytical and executive decision support information.
6. Have a method or framework with which to track the COIs performance.
7. Have a good understanding of the COIs information policies concerning security, privacy, continuity and disaster recovery

## **Relevant Frameworks**

TBD

## **Conclusion**

TBD

## References

Hamaker, Stacey. "Spotlight on Governance". Information Systems Audit Control Journal, Volume 1, 2003. 15-19.

Renner, Scott. "My Two Cats Are a Community of Interest". 2006 CCRTS.

DODI 8115.01, October 10, 2005 "Information Technology Portfolio Management".

DoD Chief Information Officer, Communities of Interest in the Net-Centric DoD: Frequently Asked Questions, 2004. [https://disain.disa.mil/nctdesc/library/COI\\_FAQ.pdf](https://disain.disa.mil/nctdesc/library/COI_FAQ.pdf).

DoD Chief Information Officer, DoD Net-Centric Data Strategy, March 2003. <http://www.defenselink.mil/nii/org/cio/doc/Net-Centric-Data-Strategy-2003-05-092.pdf>.

Proposed Outline (Slightly modified from the original)

1. Summary
  - a. Re-use part of the abstract.
2. Background and description of the problem:
  - a. A framing or portrayal of the problem (story and explanation drives home the point).
  - b. Brief literature review of COIs, Net-Centric Data Strategy to provide context, using
    - i. Past, relevant ICCRTS/CCRTS Submissions  
Renner
    - ii. ASD NII documentation/memorandum
      1. coi faq, it governance directive.
    - iii. Other relevant sources if necessary (trades, peer literature, Congressional testimony, or reports).
3. Risks to a Commercial company supporting a Defense program participating in COIs:
  - a. Relevant Threats and Risks presented in broad categories.
    - i. Using Trades/News Items/Government sources.
  - b. Table/Figure of these Risks with considerations for mitigation.
4. Relevant Frameworks to apply (Industry standards and other suggestions):
  - a. COBIT/ISACA
  - b. ISO 17799 / ISO 27001
  - c. Other suggestions (Scenario planning, Peer-Literature-Review model, Usage Fees, ect.)
5. Conclusion
6. References

---

<sup>1</sup> Renner, Scott. "My Two Cats Are a Community of Interest". 2006 CCRTS

<sup>2</sup> Hamaker, Stacey. "Spotlight on Governance". Information Systems Audit Control Journal, Volume 1, 2003. 15-19.