Network Centric Attributes Functional Team/ Net-Centric Attributes Content Work Group

US DoD Net-Centric Attributes

Invited Review Paper

Version 2.0
February 16, 2011

Lead Authors

Hans Polzer
Todd Schneider
Brenda Wilson

Contributing Authors

Aaron Budgor
Norm Day
Courtney Edwards
Mike Evanoff
Terry Longstreth
Sunita Munjal
John Reeves
Tiramule K. Ramesh
Tim Thomas
John Yanosy
Jack Zavin

Technical Editor

Beverly Brady

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

The Network Centric Operations Industry Consortium (NCOIC) Execution Plan DISA01:2007.08.02 describes the collaborative work initiated between the Defense Information System Agency (DISA) and NCOIC. DISA signed a Cooperative Research and Development Agreement (CRADA) with NCOIC to enhance understanding, development, and refinement of relevant network-centric operations (NCO) principles and practices. Through this CRADA, the United States (US) Department of Defense Chief Information Officer (DoD CIO) is engaging NCOIC to develop an industry view of the Net-Centric Attributes (NCA) developed by the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/US DoD CIO.

The execution plan was developed by DoD and DISA to fit together with the existing evolving NCOIC Interoperability Framework (NIF); Systems, Capabilities, Operations, Programs, and Enterprises (SCOPE™) Model for Interoperability; Network Centric Analysis Tool (NCAT™); and other tools and products of the NCOIC functional teams (FT), working groups (WG), and integrated project teams (IPT).

1.2 Purpose

As part of the CRADA, the DoD CIO has engaged NCOIC to develop an industry view of the implementation over time of the NCA. This NCOIC review paper documents an industry view of the DoD NCA, including a review of the NCA, recommendations for changes, and additional material to aid in the application and use of these attributes.

The intent of this work is to meet the requirements of the CRADA and to provide the larger user community with a product that can be used effectively to promote adoption of net-centricity in programs, systems, and products. There is a need for a consistent and conceptually sound evolution of NCA with the provenance to support decisions about their use and the ability to build on feedback from such use.

This review leverages the technical expertise within the NCOIC toward the development of an industry evolution plan for net-centric technologies and operations. This effort also serves to evolve the implementation of NCO across a more diverse constituency and better inform all stakeholders, including NCOIC member companies, defense, government and non-government organizations, and other large organizations. When called on to make decisions about which technologies to employ, or what best enables net-centric behavior, these stakeholders will be better able to interpret these attributes in their particular context, their assessment context.

1.3 Approach

The approach represented in this paper was designed to meet the objectives described in the CRADA. It includes providing a product back to the DISA and DoD and developing results that provide benefit to NCOIC and its members. Part of this approach involved a workshop held 18-19 August 2009 in Crystal City, Virginia, with members of the NCOIC, Jack Zavin, and other US DoD representatives. The goal of the workshop was to examine the intent of the attributes as written (see Table 2) and then analyze the attributes with the following criteria in mind:

- Attributes need to be
  - Usable (ideally measurable)—Goal oriented (i.e., intent).
  - If not measurable, then qualifiable in a repeatedly consistent fashion.
  - Effective (i.e., provide value to the user)—A quantifiable benefit.
  - Understandable—Terminology needs to be not too different from current vernacular.
  - Grounded in a way to have temporal stability.
  - Easily transformed into context specific equivalents.
- Provenance—Each attribute needs a well documented pedigree providing the basis, rationale, and context of usage or applicability.

It was during this workshop that the majority of NCOIC recommendations were created.

With these objectives and approach in mind, this review paper is structured as follows. First, the DoD NCA are described in their original form. The context for their creation and intent is described. The NCA are reviewed for perceived intent and understandability and then critiqued. Based on the review and critique, recommendations are provided. These recommendations range from possible rewording to alternative attributes. Following the critique of the attributes, general observations and missing attributes are addressed. In addition, to provide users with guidance on the use and applicability of the attributes, a discussion of assessment contexts is given.

As part of the NCOIC analysis, the DoD NCA are mapped to NCOIC Core Net-Centric Principles. These NCOIC principles represent the fundamental aspects of a net-centric environment, its primitives or axioms, independent of any particular operational or organizational context. The principles help to lay the basis for attribute evolution/devolution and facilitate the realization of the net-centric vision of interoperating capabilities with fewer constraints as a result of nationality, operational domain, or organizational affiliation.

1.4 Scope – Technical vs. Nontechnical

The DoD NCA focus on the technical properties of systems needed to support net-centricity, although many of these properties also have operational, cultural, and business model implications and relations. The other non-technological properties needed to support operations are not a focus of the current set of DoD NCA[1]. NCA beyond technology-driven attributes are kept distinct in this review task, but do arise in the comparison with the various NCOIC net-centric principles and attributes that exist in NCOIC documents, since these include a number of attributes that are not purely technical in nature. Recommendations regarding incorporation of some of these non-technological properties in the set of DoD NCA could be incorporated with the current technically oriented perspective at a later time (see Section 3.11.3.2).

1.5 Definitions

Table 1 lists the definitions of key terms used within this document. These terms, along with their definitions, are recommended for inclusion in the NCOIC Lexicon.

[1] After this review was underway, a Human Interoperability attribute was added to the original nine (Section 3.11.2).

Table 1. Definition of Terms

Term	Definition
Principle	A basic generalization that is accepted as true and that can be used as a basis for reasoning or conduct.
Net-Centric Principle	A basic context-independent generalization about the net-centric environment that is accepted as true and can be used as a basis for reasoning, attribute selection, or organizational structure.
Attribute	A feature or characteristic whereby objects or individuals can be distinguished and that admits qualification or quantification.
Net-Centric Attribute	An attribute that characterizes an aspect of the net-centric environment relevant for a system, service, product, capability, or organization in that environment.
Attribute Assessment Context	The surroundings, circumstances, environment, purpose, background, or settings that determine, specify, or clarity the application of one or more attributes.

1.6 Acronyms and Abbreviations

The following acronyms are used in this review paper.

ASD	Assistant Secretary of Defense (US DoD)
CIO	Chief Information Officer
COE	Common Operating Environment
COI	Community of Interest
CRADA	Cooperative Research and Development Agreement
DHS	Department of Homeland Security
DISA	Defense Information System Agency
DNS	Domain Name Service
DoD	Department of Defense
FT	Functional Team
GIG	Global Information Grid
HI	Human Interoperability
HTML	Hypertext Markup Language
IA	Information Assurance
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPT	Integrated Project Team
IT	Information Technology
JCIDS	Joint Capability Integration and Development System
KPP	Key Performance Parameters
NATO	North Atlantic Treaty Organization
NC	Net-Centric

NCA	Net-Centric Attributes
NCAT	Network Centric Analysis Tool
NCOIC	Network Centric Operations Industry Consortium
NCO	Network Centric Operations
NCP	Network Centric Pattern
NIF	NCOIC Interoperability Framework
NII	Networks and Information Integration (US DoD)
NNEC	NATO Network Enabled Capability
OSD	Office of the Secretary of Defense (US DoD)
QoS	Quality of Service
SATCOM	Satellite Communications
SCOPE	Systems, Capabilities, Operations, Programs, and Enterprises
TCP	Transmission Control Protocol
UAV	Unmanned Aerial Vehicle
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
US	United States
USAA	United Services Automobile Association
VOIP	Voice Over Internet Protocol
WG	Working Group

2 ASD(NII)/DoD CIO Net-Centric Attributes

2.1 History and Background

The NCA[2] evolved from an initial publication in 2004 as one part of an effort to describe NCO. Another part of this effort was the Net-Centric Checklist[3]. The NCA originally covered what the ASD(NII)/DoD CIO during that time called his regulatory regime and was given an initial title of Net-Centric Tenets. The intent of the NCA was to provide a filter, albeit coarse, for looking at US DoD investments so that, if warranted, emphasis could be placed on those that supported the US DoD's evolution into the information age.

The NCA and Net-Centric Checklist evolved under an effort to provide a concise depiction of a net-centric environment through engagement within and external to the US DoD. The NCA list was made official in 2006 and posted on the ASD(NII)/DoD CIO's public Web site. The NCA are used along with other documents in internal event-driven net-centric reviews.

The evolutionary timeline of the NCA into the current form is as follows.

1. 2004—The ASD(NII)/DOD CIO publishes the initial set of NCA, containing net-centric tenants and a net-centric checklist. The purpose of the list was to provide a way of looking at US DoD investments so that emphasis could be placed on those that supported the US DoD's evolution into the information age.

2. 2006—An updated version of the NCA was published. The revisions were intended to expand the scope beyond the US DoD and to make the attributes useful in event-driven net-centric reviews.

3. 2007—A critique of the attribute approach entitled Beyond Technical Interoperability was presented at the NCOIC Advisory Council and Executive Council Meeting in September 2007 by Jack Zavin, Associate Director, Deputy Assistant Secretary of Defense C3S2. The critique focused on defining stakeholder context for attribute evaluation. The paper defined the following classes of functional entities, shown in Figure 1, that interact with net-centric systems:

    a. Managers/Operators.

    b. Information Producers/Publishers.

    c. Information Service Providers.

    d. Information Transport Providers.

    e. Users/Consumers.

[2] http://nesipublic.spawar.navy.mil/nesix/Frames/G1002
[3] http://cio-nii.defense.gov/docs/NetCentric_Checklist_v2-1-3_.pdf

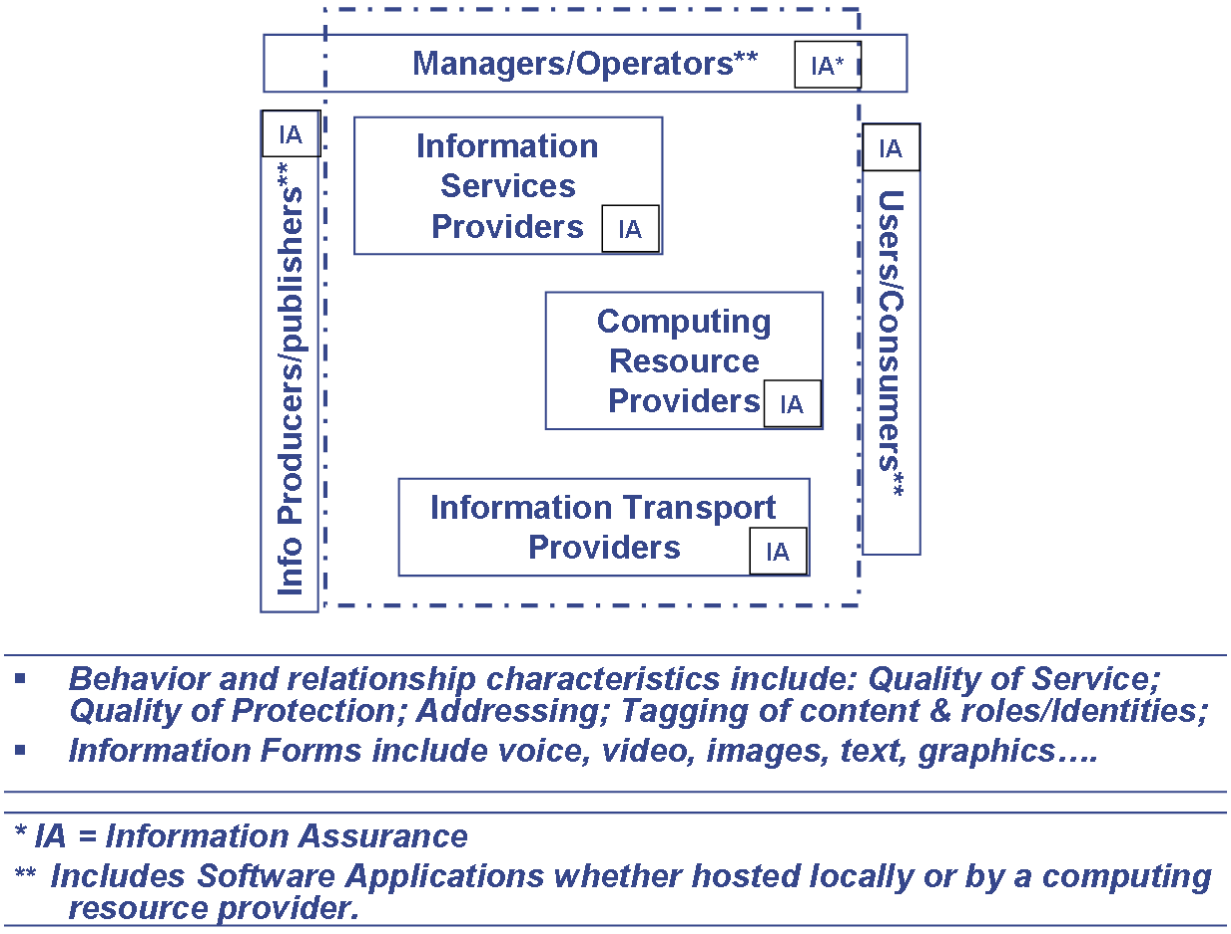

Figure 1. Functional Entities

Each functional entity has a different perspective on the system, and thus takes a different approach to evaluation of NCA. These different perspectives are now referred to as assessment contexts. They are used to provide additional context for the application of one or more attributes. The contexts provide the interpretive constraints needed to allow qualification/quantification of the attribute(s).

This paper generalizes the approach of using functional entities to provide context for evaluations, assessment context. Our evaluation of the NCA includes identification of the possible assessment contexts of the attribute, and how that might change the degree of specificity or applicability of the attribute. The assessment context provides background and context for application of an attribute, and thus focuses evaluation of the net-centric system with respect to its intended use, and not just to some abstract set of NCA that apply universally. Assessment contexts, their dependencies, and their use in assessing the degrees of net-centricity are described in Section 5.

2.2 Description

The DoD's NCA have evolved from an original set published in 2004 and merge much of the interface specifics with behavior of networks and services to provide a greater understanding of quality of service, quality of information, and ultimately quality of operation. In addition, these NCA span the wide range of information forms including voice, video, imagery, text, and graphics, and rely on robust role

and identity management mechanisms to ensure trusted relationships exist among networked entities. The DoD NCA[4] are given in Table 2.

Table 2. ASD(NII)/DoD CIO Net-Centric Attributes

Attribute	Description
Internet & World Wide Web Like	Adapting Internet & World Wide Web constructs and standards with enhancements for mobility, surety, and military unique features (e.g., precedence, preemption).
Secure & Available Information Transport	Encryption initially for core transport backbone; goal is edge to edge; hardened against denial of service
Information/Data Protection & Surety (built-in trust)	Producer/Publisher marks the info/data for classification and handling; and provides provisions for assuring authenticity, integrity, and non-repudiation.
Post in Parallel	Producer/Publisher make info/data visible and accessible without delay so that users get info/data when and how needed (e.g., raw, analyzed, archived).
Smart Pull (vice smart push)	Users can find and pull directly, subscribe or use value added services (e.g., discovery). User Defined Operational Picture vice Common Operating Picture.
Information Data Centric	Information/Data separate from applications and services. Minimize need for special or proprietary software.
Shared Applications & Services	User can pull multiple applications to access same data or choose same apps when they need to collaborate. Applications on desktop or as a service.
Trusted & Tailored Access	Access to the information transport, info/data, applications & services linked to user's role, identity & technical capability.
Quality of Transport Service	Tailored for information form; voice, still imagery, video/moving imagery, data, and collaboration.

2.3 Application

2.3.1 US Department of Defense

The nine NCA continue to serve as a coarse filter in assessing net-centric programs and proposed solutions. However, the NCA have not been applied consistently across DoD. The motivation for the attributes from DoD's perspective has been a need for an acquisition assessment tool. Such a tool needed to be simple and have continued applicability as technology advanced. Such a tool would incorporate the assessment context to provide the appropriate interpretation and level of detail needed to simplify the task of assessing compliance, similar to the NCOIC NCAT™ tool.

[4] http://cio-nii.defense.gov/sites/coi/Governance/NetCentricAttributesOfficial.pdf

It should be noted that application or use of the NCA can be in contexts and for purposes other than evaluating a specific DoD system or design. For example, NCA can be applied during concept development and requirements definition to help structure a capability in ways that makes it more readily fit into a net-centric environment, rather than to have some "net-centric" requirements "tacked on" at the end of the requirements definition process as an afterthought. NCA also can be used to guide post-deployment upgrades/changes to existing systems, including changes to implement or improve interoperability with systems external to the sponsoring Service or even external to the DoD. In such cases, the DoD NCA might have counterparts that are similar to, but not identical to the DoD attributes (e.g., NATO's Network Enabled Capability [NNEC]), which the sponsor of the external systems applied to those systems during their development. In such applications, the NCA may need to be tailored to suit the scope and context in which the systems are being used. If an evaluation using the NCA is conducted, then it may be for purposes other than compliance with the DoD's requirements (and contexts). However, throughout this paper, the term assessment context is used to include all such non-evaluation type uses of the NCA for convenience.

2.3.2 NCOIC

The review of the NCA and associated analysis under this task provides another impetus toward the integration of SCOPE™ [5] and NCAT™ [6] content. NCOIC has been engaged in integrating the SCOPE™ and NCAT™ questions to meet the goals of NCOIC. The intent of the integration is to simplify the task of using both SCOPE™ and NCAT™ in developing net-centric systems.

2.3.3 Industry

The application of the NCA as currently expressed poses a challenge to industry. The NCA can be interpreted in varying ways depending on the context, person, or organization doing the interpreting. The functional entities were intended to provide context in the use of the attributes for actual evaluations. But the functional entities decomposition provides only one aspect of context that needs to be considered when applying NCA, and is focused on characterizing different DoD stakeholder types. The functional entities by themselves provide insufficient guidance for consistent and appropriate evaluations by industry developers of systems.

Industry may want to apply NCA in internal research and development contexts, in different developmental phases, and during post-deployment life-cycle support contexts. An attribute worded in a very general, abstract way for application in a DoD acquisition decision context would need to be tailored or translated into more design- and domain-specific wording, making it understandable to system engineers and software developers for the type of system in question and for the life-cycle phase at which the system is being evaluated. For example, Secure and Available Information Transport means something quite different to a back-office information technology application developer than it does to a UAV system developer. Characterizing this attribute in a way that each of the developers for these different system types can understand and use requires tailoring specific to each program or assessment context. Likewise, how to evaluate whether a system meets the Information/Data Protection and Surety (Built-in Trust) attribute depends critically on where that system is in the development life cycle (e.g., system requirements review, preliminary design review, critical design review, factory acceptance test, etc.) and on what security domain(s) it is intended to operate in (e.g., tactical data links, classified networks or open Internet).

[5] https://www.ncoic.org/technology/deliverables/scope/
[6] https://www.ncoic.org/technology/activities/education/ncat/

As part of this review, an expanded and more detailed description of assessment contexts is provided (see Section 5). The description of the contexts provided is by no means complete. The intent is to provide a sufficient set of top-level assessment contexts from which others may be derived consistently.

3 Review, Critique, and Recommendations

The NCOIC understands that the intent of the NCA was to simplify evaluations of the net-centricity of systems or programs within the DoD. The NCOIC also understands that in proposing the NCA, there was not an attempt to mask the underlying complexities of NCO, but rather to provide a simpler and less intimidating way to access NCO complexity (in the context of acquisition). With these goals in mind, this review paper expands on these premises by clearly identifying the aspects aggregated in an NCA. These additional aspects are described in the following NCA critiques as intent: What are the aggregated aspects represented by the NCA?

A net-centric environment is by its very nature highly interrelated and interdependent. Any attempt to simplify a complex and highly interrelated environment necessarily requires the aggregation of multiple concepts or their relationships. To apply these attributes within the original intent and make them more useful overall, the underlying concepts and their relationships need to be identified. In the context of NCOIC, such an exposition (in a future extension of this work) also requires a connection or mapping to the relevant SCOPE™ dimensions and NCAT™ questions or profiles.

The critique of the attributes is structured as follows: a restatement of the attribute, background information about the attribute, then a discussion of the intent of the attribute[7], followed by a review of the attribute, and finally recommendations related to the attribute. The recommendations may be suggestions about rewording or may be suggestions on one or more candidate replacement attributes. In most cases, the candidate replacement attributes are more technology independent and less domain specific in their wording than the original attributes. These changes may make them less easily applied in some assessment contexts and more easily applied in other assessment contexts. Ultimately, the attributes will need to be refined to different levels of granularity and specificity depending on the assessment context in order for them to be useful (discussed further in Section 5). The candidate replacements offered here are worded in a way to have appeal and applicability beyond a DoD context and still be useful in the early development/acquisition phases of a system or capability.

3.1 Attribute 1: Internet and World Wide Web Like

Adapting Internet & World Wide Web constructs & standards with enhancements for mobility, surety, and military unique features (e.g., precedence, preemption).

3.1.1 DoD Background

The term *Internet* is used to refer to the transport infrastructure while the *World Wide Web* refers to the data content that is carried by the Internet.

[7] The intentions of the attributes were developed during a workshop held 18-19 August 2009 in Crystal City, Virginia.

3.1.2 NCOIC Review

3.1.2.1 Intent

The perceived intentions of this attribute are as follows:

- Open-endedness/extensibility—Among the properties of the Internet constructs[8] is its extensibility or open-endedness.
- Recognition of self and acknowledgement of others—Design awareness of other systems (e.g., globally unique identifiers).
- Unbounded reach—The ability to find and use information without a priori bounds.
- Decoupling information from transport—In identifying both the Internet and the World Wide Web, a clear distinction should be inferred between the information available and the mechanisms to transport it.
- Ubiquity of related/accessible/addressable entities—A user/consumer view of availability that is independent of time and location.
- Ability to identify or distinguish entities—Among the constructs of the Internet/Web is the use of identifiers (URL, URI, and URN) to help distinguish entities in the environment.
- Production Rule approach to standards—Internet Engineering Task Force (IETF) model: use of standards in the context of behaviors of individual entities as opposed to top-down dictates of specific nodal architectures or designs.

3.1.2.2 Critique

A key issue here is to what degree DoD actually wants to leverage the Internet and World Wide Web as opposed to creating a facsimile thereof inside the DoD intranet (i.e., the Global Information Grid [GIG]). Enhancements make sense inside the DoD intranet, but are more problematic on the open Internet, requiring much more social engineering. The other issue is that the attribute as stated only hints at what would make the GIG and its systems/services Internet and World Wide Web like—what are the attributes of the Internet and the Web that DoD wants to emulate here? Clearly, there are some attributes that are not desirable for DoD. For example, the Internet today treats each requestor of transport services the same and does not distinguish between high or low priority users, although there are some mechanisms to support different quality of service (QoS) levels based on traffic type, such as voice over IP (VOIP). And security was not a major consideration in early Internet protocol development. But the attribute as stated does not focus on the desirable properties, leaving it up to the appliers of the attribute to figure out for themselves what these might be in their particular context.

- Three very different areas are referred to together: mobility, surety, and military unique. These could be addressed separately under sub-attributes or distinguished using application contexts.
- Remove the words starting “with enhancements…”. As an attribute, whatever the enhancements should be, should have been prescribed.
- Provide a better description of Web like—such as explicit, but indirect/symbolic addressing (i.e., DNS), no a priori enterprise/network boundary or control assumptions, no a priori system or

[8] See *Architectural Principles of the Internet*, tools.ietf.org/html/rfc1958.

enterprise architecture assumptions other than TCP/IP support, open protocols for accessing services, dynamic connection to services (no separate offline agreements to negotiate and sign or get approved before being able to connect) minimal a priori information model assumptions (HTML and URLs).

3.1.3 NCOIC Recommendations

Based on the comments stated in Section 3.1.2.2, and to meet the intent of this attribute yet move closer to the underlying aspects addressed as identified in the section on intents, the following replacement attributes are recommended.

3.1.3.1 Candidate Replacement(s)

The following candidate replacement attributes were arrived at after discussion of the original attribute. The important points of these discussions are listed in Sections 3.1.2.1 and 3.1.2.2. These candidate replacement attributes represent the consensus as to the necessary underlying capabilities described in the original attribute. Media independence represents just that, information not coupled to a particular transport media or mechanism (i.e., proprietary media – Link-11, Link-16, RS-232 connections, particular waveforms, etc.). Open-ended pervasive accessibility is a fundamental capability of the World Wide Web. However, not all information accessible over the Internet is freely shared, nor is all information potentially accessible through institutional "intranets" made accessible over the public Internet without additional information access controls. Last, open standards based is another core aspect of the World Wide Web. It allows the commonality needed to share information, but also supports access controls to enable controlling with whom the information and services might be shared.

- **Media Independence**—Information used, produced, published, or disseminated by the service(s) or system(s) is decoupled from transport mechanisms.
- **Open-Ended Pervasive Accessibility**—The system(s) or service(s) has the ability to find, use, and control information and services (which requires an ability to identify and distinguish entities and the publication of information with minimal a priori constraints).
- **Open Standards[9] Based**—To support interoperability programs/projects, systems, and services must maximize the use of openly available and unencumbered technical and process standards that support media independence, pervasive accessibility, and trustworthy control of access to information and services.

3.2 Attribute 2: Secure and Available Information Transport

Encryption initially for core transport backbone; goal is edge to edge; hardened against denial of service.

[9] Recommendations for selection and promotion of open standards in net-centric contexts is contained in the NCOIC working document: Baseline Approach for a Standards Management Framework, NCOIC-SMF Baseline-20100329v1.0.

3.2.1 DoD Background

This attribute refers to the security and availability needed for information transport.

3.2.2 NCOIC Review

3.2.2.1 Intent

This attribute encompasses several aspects or attributes. The perceived intentions of this attribute are as follows:

- Secure communication edge-to-edge[10] and/or end-to-end[11].
- Protection of transport mechanisms against denial of service or any attack that impedes communications or loss of assets/resources.
- Distinction between protecting the transport and protecting the content.

3.2.2.2 Critique

As written, the attribute appears to be a solution. Different operational purposes suggest differing degrees of availability and security in data transport. The open Internet supports different levels of transport security and assured delivery for different purposes (e.g., video streaming). The intent of this attribute is to push for ubiquitous transport service availability and for ease of a user to obtain protection for transport services. An example of this might be encryption services that don't have to be invoked or applied internally to application logic. Another example is being able to select the level of protection desired or appropriate as a by-product of connecting or sending information to some other network agent or user.

- This seems to be a one-size fits all—what are the specific attributes needed?
- Are there other ways to accomplish secure information transport? Encryption is a solution and should not be in an attribute.
- Can the levels of security be tailored to the nature of the participants involved in the communication?
- This implicitly includes ubiquity of access. To make use of available transport services, there must first be access to these services.
- This represents availability from the end-user perspective (i.e., denial of service).
- This attribute is more about the GIG/available infrastructure than an arbitrary program or capability.
- Aspects of the interaction between the transport and content services is not addressed.
- There is no distinction between the consumer/producer view and the transport services provider view.

[10] "edge-to-edge" refers to a (spatial) location view of the communications path (i.e., the two locations of the end points) consistent with a transport view.
[11] "end-to-end" refers to a consumer-producer view of the communications path (i.e., the two application end points) consistent with an information or content view.

3.2.3 NCOIC Recommendations

- Distinguish the required capability or capabilities and their attributes—secure and available end-to-end information transport might be the desired capability.
- This attribute requires an application context to distinguish its interpretation. Most individual systems or programs/projects (that are not explicitly about communications infrastructure) would exhibit this attribute by using available secure transport services, as opposed to developing or providing them as part of their system scope, or by taking advantage of data protection services when they are needed/appropriate.

3.2.3.1 Candidate Replacement

The following candidate replacement attributes were arrived at after discussion of the original attribute. The important points of these discussions are listed in Sections 3.2.2.1 and 3.2.2.2. The goal of the candidate replacement was to facilitate the application of this attribute. As noted, most systems make use of existing or extra-system security capabilities and do not develop their own. The candidate replacement separates the responsibilities of providing the different components needed to meet the intent of the original attribute.

NCOIC recommends that this attribute description be restated as follows and that it be used in system design/architecture assessment contexts:

- **Protected and Assured Transport Services**
  - The program/project, system, or service makes use of existing (i.e., available and external to the program/project, system, or service) specified assurance, protected, and defended transport services where feasible/available.
  - The infrastructure systems provide specified assurance, protected, and defended transport services that are accessible and available wherever and whenever needed.

3.3 Attribute 3: Information/Data Protection and Surety (Built-in Trust)

Producer/Publisher marks the info/data for classification and handling; and provides for assuring authenticity, integrity, and non-repudiation.

3.3.1 DoD Background

Information assurance (IA) appears in four of the nine attributes. It is addressed as a key part of each of these attributes and is not called out separately because of its integral nature.

3.3.2 NCOIC Review

3.3.2.1 Intent

The perceived intentions of this attribute are as follows:

- To be inclusive of handling and distribution markings that support use/or distribution-control paradigms.
- Data quality preservation and measurement.
- Separating data security controls from the application services.
- Tagging of data at the source for integrity and surety.
- Protecting data at rest and in motion.

3.3.2.2 Critique

As written, this attribute implies a solution. IA metadata exists to address this area. The attribute tries to capture or describe the degree to which information providers take ownership of security awareness and compliance, as well as responsibility for labeling data or services they provide from a security perspective—as opposed to simply assuming they are operating system high and that someone else (i.e., the network/platform provider) has responsibility for perimeter security or the labeling of data.

The attribute also represents a constraint on net-centric behavior (otherwise there would be no need for any restrictive markings). The attribute recognizes implicitly that not all data are shared or sharable with everyone on the network. And not all service users are benign or authorized to access all services. The dynamics of a net-centric environment require that network entities examine the credentials of requestors for services or data to demonstrate the requestor's rights to access the data or services or to establish a longer term relationship (e.g., create a session or request a user ID or profile). Part of that relationship typically includes any data labeling or protection rules that apply in the context of that relationship.

Different systems and applications may require different levels of net-centricity (e.g., intelligence data would not be shared as openly as medical or general logistics information). The presentation of the NCA should provide guidance in identifying which attributes are necessary to meet different levels of net-centricity and interoperability, which could be accomplished with a more complete description and application of assessment contexts.

3.3.3 NCOIC Recommendations

Two recommendations have been proposed:

- One suggestion is to delete "marks the info/data for classification and handling; and ."
- An alternative rewording might be the following: "Systems and services take responsibility for establishing and maintaining appropriate trust relationships with users and other services on the network (leveraging available network/enterprise security services). Systems and services take measures to comply with any security labeling, data protection, and access control requirements entailed by the trust relationships that they commit to, and monitor the environment to ensure that conditions on which the trust relationships were established have not changed (e.g., revocation of certificates)."

3.3.3.1 Candidate Replacement

The following candidate replacement attributes were arrived at after discussion of the original attribute. The important points of these discussions are listed in Sections 3.3.2.1 and 3.3.2.2. The goal of the candidate replacement attribute was to identify clearly the underlying concept of trust relationships

and distinguish what a trust relationship entails. NCOIC recommends that this attribute description be restated as follows:

- **Producer/Publisher Trust Relationships [with users and services]**
  - The program/project, system, and/or service(s) have mechanisms for establishing and maintaining appropriate trust relationships with users and services on the network.
  - The program/project, system, and/or service(s) take measures to comply with those security labeling, data protection, and access control requirements entailed by the trust relationships and monitor the environment to ensure that conditions on which the trust relationships were established have not changed (e.g., revocation of certificates).

3.4 Attribute 4: Post in Parallel

Producer/Publisher make info/data visible and accessible without delay so that users get info/data when and how needed (e.g., raw, analyzed, archived).

3.4.1 DoD Background

This attribute addresses the data needs of critical operations with increasingly large real-time data sources. DoD wants to make all data available via pull so that systems could use it for their own purposes without encumbering the information/data producers with additional requirements.

3.4.2 NCOIC Review

3.4.2.1 Intent

The perceived intentions of this attribute are as follows:

- Be able to support operational timeline requirements (for information).
- Break cultural boundaries and ownership controls over information.
- Get programs/projects (information producers/publishers) to anticipate nontraditional users of their information or data.
- Provide additional contextual data allowing use (of data/information) by a larger community.
- The attribute suggests that producers and publishers need to look downstream toward the end users, implying the need for attention to behavioral aspects.

3.4.2.2 Critique

Post in parallel is a data distribution/dissemination strategy, not an NCA per se. Post in parallel is not always an appropriate strategy, especially if the raw data contains insufficient context for appropriate discovery or proper interpretation by a consumer not familiar with the data source (i.e., the producer or publisher's context or intent). It also may not be appropriate [to post in parallel] when the data collection platform is not well connected [to the GIG] or does not have the capacity to scale necessary to support requestors for the posted data. It may be difficult for the producer/publisher to know the needs of all user groups, thus imposing unrealistic resource obligations on the producer/publisher.

Additional issues include the following:

- Conflict with data understandability (e.g., loss of collection source).
- Tradeoff between timeliness and understandability.
- Overlap with the "information/data protection and surety" attribute.
- An assumption that additional data processing may take place (hence the need for posting in parallel).
- The current title has specific meaning and may not properly convey the intent.

3.4.3 NCOIC Recommendations

- The attribute, as stated, may be understood as an ideal end state. However, it is difficult to achieve and impractical in some circumstances. The entailed network management requirements could be massive and would be constrained by pragmatism.
- The following rewording is suggested: "Make data accessible over the network—Producer/Collector/Publishers make information they collect or produce discoverable and accessible over the network in a manner and timeframe appropriate to the nature of the information and its potential value to other entities on the network."

3.4.3.1 Candidate Replacement

The following candidate replacement attributes were arrived at after discussion of the original attribute. The important points of these discussions are listed in Sections 3.4.2.1 and 3.4.2.2. The candidate replacement attribute reflects the need to account for the type and context of the data to be made available. In particular the context of the information access includes the trust relationship between the provider and consumer (which may be dynamic, see Section 3.3.3.1). The specific relationships among consumer and provider will determine the manner and timeframe appropriate for accessibility. NCOIC recommends that the attribute title and description be restated as follows:

- **Post data/information for network access**—The program/project, system, and/or service(s) have made their products discoverable and accessible on the network in a manner and timeframe appropriate to the nature of the information/data.

3.5 Attribute 5: Smart Pull (vice Smart Push)

Users can find and pull directly, subscribe or use value added services (e.g., discovery). User Defined Operational Picture vice Common Operational Picture.

3.5.1 DoD Background

This attribute reflects the historical need for pull over conventional push or broadcast information dissemination mechanisms. Both are needed depending on the circumstances.

3.5.2 NCOIC Review

3.5.2.1 Intent

The perceived intentions of this attribute are as follows:

- The ability for a user to obtain the right information at the right time. Obtain may be via "smart pull"—wherein users search/discover/retrieve per their imminent declared needs. Or obtain also may be via "smart push"—wherein policy, context, or persistent search send data to users without imminent user request or need.
- Empower the information consumer with respect to the information provider.
- Change the information providers' culture to account for information consumers (i.e., understandability, timeliness). Maximize the utility of communication infrastructure by increasing end-user intent in fractional bandwidth usage.

3.5.2.2 Critique

This attribute appears to reflect the current paradigm of publish and subscribe and suggests a false dichotomy. Both smart push and smart pull strategies are appropriate information/data distribution/dissemination strategies. Neither is inherently more net-centric than the other. Rather, net-centric behavior recognizes different stakeholders and operational contexts require different strategies appropriate to achieve operational effectiveness. Therefore, data producers/providers/publishers should support multiple types of interactions that allow users to subscribe to smart push services as well as perform dynamic search/discovery and smart pull data access.

Conversely, providing data to any user (on the GIG) incurs costs to the data provider/producer/publisher, the transport provider, and others on the network (e.g., reduced resources). These costs should be visible to the requestor. This visibility would help minimize casual/inappropriate requests to provide or use data or services that are expensive to deliver.

3.5.3 NCOIC Recommendations

- This attribute should be combined with Attribute 4: Post in Parallel as a single attribute. For instance, "Make information/services accessible over the network—users/applications can find and pull data directly or subscribe to specific data providers/services appropriate to their operational context and needs, and also see the cost/impact on the information provider."
- This attribute also should address the means to negotiate specific information access arrangements and that the mechanisms [for negotiation] be provided by systems/service sponsors and developers, ideally executable over the network.

3.5.3.1 Candidate Replacement

The following candidate replacement attributes were arrived at after discussion of the original attribute. The important points of these discussions are listed in Sections 3.5.2.1 and 3.5.2.2. The candidate replacement attribute reflects the underlying intent of smart push and smart pull and goes beyond that to cover the ability of users to have sufficient context to correctly use information provided and for information producers to account for change—the ability to adapt. Information providers and users should establish as much of their shared context as possible to enable adaptive access mechanisms

appropriate to their operational relationship. NCOIC recommends that the attribute title and description be restated as follows:

- **Adaptive Information**—The system and/or service(s) has the ability to easily include new sources of information, in new formats and exchanges, with new or different security techniques and has provided users and services access to its information and data in ways most appropriate for their shared context while allowing users to negotiate access arrangements and understand the associated costs.

3.6 Attribute 6: Information/Data Centric

Information/Data separate from applications and services. Minimize need for special or proprietary software.

3.6.1 DoD Background

This attribute includes behavioral aspects as well. The goal was to divorce the information from particular or proprietary applications or data schemes involved in its production or use.

3.6.2 NCOIC Review

3.6.2.1 Intent

The perceived intentions of this attribute are as follows:

- Make information more accessible (by decoupling it from applications that are used to find or view it).
- Motivate programs/projects to make their information more widely accessible and usable.
- Remove the necessity for a common application that must be distributed to all possible users and be able run on all user platforms.
- Agility—The ability to use information dynamically (e.g., mash-ups) with minimal pre-conditions (e.g., common application).

3.6.2.2 Critique

The first sentence stands alone. Given the meaning of the first sentence, the title appears a bit unclear. This attribute may provide additional value if it can be extended to more than data—to all layers of the Open System Interconnection Reference Model.

This attribute reflects a net-centric tenet and a design principle—separation of concerns. This attribute also implicitly conflicts with the notion of data access services. Such services inherently constrain the way the information is made accessible over the network and by the exposed information model (i.e., there may be additional aspects of the information model not exposed).

This attribute originally was intended to get system/application developers to make data available over the network separate from a particular application user interface/client. It is somewhat redundant with the

previous two attributes (Attribute 4: Post in Parallel and Attribute 5: Smart Pull (vice Smart Push)) and should simply be rolled into the "make data accessible over the network" attribute.

Potentially, this attribute could be amplified with the phrase "make the frames of reference used (i.e., context) and scope assumptions of information/data access services explicitly visible/accessible over the network as well." To reinforce the point about application independence add "data access mechanisms over the network and the information models and frames of reference used to represent the information/data should not be dependent on access to any specific user application or proprietary program."

3.6.3 NCOIC Recommendations

This should be expressed as one attribute—make information accessible over the network, with three different areas of emphasis that stress the main factors that have inhibited this accessibility in the past: not publishing data in a timely fashion, not supporting dynamic subscription or discovery service, and burying data inside applications and application user interfaces where it cannot be accessed over the network.

3.6.3.1 Candidate Replacement

The following candidate replacement attributes were arrived at after discussion of the original attribute. The important points of these discussions are listed in Sections 3.6.2.1 and 3.6.2.2 The candidate replacement attribute makes explicit the intent of the original attribute by requiring a clear and distinct separation of data and information from its sources and requiring context information to allow potential users a more complete understanding of the information—providers should provide as much explicit representation of user and data/information attributes or markings as possible to enable appropriate controls and visibility. NCOIC recommends that the attribute title and description be restated as follows:

- **Information and Data Independence**—The program/project and/or system has separated its information and data from applications and services (dependencies) and has provided with sufficient context (e.g., metadata, business rules, operation name, training program) to enable users to use the information/data correctly for their purposes.

3.7 Attribute 7: Shared Applications and Services

Users can pull multiple applications to access same data or choose same apps when they need to collaborate. Applications on 'desktop' or as a service.

3.7.1 DoD Background

This attribute includes behavioral aspects. It is an attempt to discriminate between an application and a service—installed on a desktop, it is an application; accessed remotely, it is a service. This attribute attempts to describe sharing of applications, the associated costs, and the reuse of applications and services.

3.7.2 NCOIC Review

3.7.2.1 Intent

The perceived intentions of this attribute are as follows:

- Support of self-synchronization.
- Differentiate applications from (network accessible) services.
- Reuse software as services over a network connection (i.e., client platform independent).
- Decoupling of capability from implementation technology choices.
- Allow multiple users to share application content/state and collaborate with each other via the application.
- These definitions convey the notion that an application is a software application whose majority of code runs on a machine directly interacted with by the user (i.e., a physical proximity of the user and the running software), whereas a service has the bulk of its code or software running on a machine that is accessed over the network (i.e., may not be in physical proximity to the user).

3.7.2.2 Critique

The title suggests a common operating environment (COE) and the intent overlaps with data independence. This attribute, as stated, adds nothing to what is covered in data independence: if there is data independence, then no single application is required to use or access the data. Hence, multiple applications can share the data. Moreover, the ability to assess conformance in the context of a particular program/project or system seems dubious. Who would be providing the multiple applications?

The second sentence of the description, “Applications on ‘desktop’ or as a service” is an information technology paradigm or architectural approach to an enterprise and not an attribute of a particular program/project or system. It may be asked of a particular program/project or system whether it is providing an application as a service, but providing all applications as a service seems questionable. The description requires users pull while the second sentence is limiting and somewhat dated. This attribute attempts to encourage or incentivize development of collaborative applications. This is a fairly complex topic and may be difficult to characterize succinctly as an attribute.

If the intent of this attribute is about application/service access and use in a net-centric environment, then it should be reworded properly to reflect that. For instance, “Program/project/system applications can be used as services over the network.”

It also is related to the previous attribute, Information/Data Centric, in that many applications assume a single user data state, context, or description of reality. So this attribute is trying to make applications more inherently multi-user; to encourage different applications to share a data state among multiple users that wish to collaborate. This necessitates both making data accessible separate/decoupled from the user client applications, as well as explicit representation of the data state—its scope, context, or frame of references. This is generally a good idea although, as stated, it does not reflect the additional data needed to support a multi-user/collaborative environment and may not be an NCA that systems/services should exhibit. Perhaps rewording such as “net-centric services and applications should support multiple simultaneous users and optionally allow the users or applications to share state values with each other, if appropriate to the application service” would be appropriate.

3.7.3 NCOIC Recommendations

- This attribute should be dropped. The attempt to distinguish between application and service is contrived and unconvincing. The choice of computer host for a software function is irrelevant except where requirements for physical proximity or communications latency are insurmountable obstacles to providing transparent access to authorized processes. To the degree that such constraints are inherent in the environment or architecture, the actualization of a net-centric context is constrained correspondingly. Conceptually, the location of services that provide specific functions should be opaque to invokers of those functions. If system performance, security, or response time requirements cannot be met without physical allocation of functions to specific resources (e.g., processors), then those functions should be identified explicitly as being outside of the net-centric framework.
- If not dropped, then the attribute should be refocused on the ability of applications to be available as services that can be accessed easily (e.g., the capability or application is available as service accessible from a standard desktop computer). If applications are accessible as services and there is data independence, then the ability to collaborate with the same application applied to the same data follows.
- NCOIC further recommends that definitions be developed to distinguish between applications and services.

3.7.3.1 Candidate Replacement

NCOIC believes the intent of this attribute can be met by the candidate replacement attributes of Adaptive Information Access (Section 3.5.3.1) and Information and Data Independence (Section 3.6.3.1) and has no candidate replacement recommendations for this attribute.

3.8 Attribute 8: Trusted and Tailored Access

Access to the information transport, info/data, applications & services linked to user's role, identity & technical capability.

3.8.1 DoD Background

IA is included explicitly in this attribute. This attribute is trying to address several aspects of user attributes, including user attributes from the perspective of permissions (i.e., role, need to know, etc.), attributes related to the user's client technology (e.g., a smart phone, laptop, etc.), and user context (e.g., working in an unsecured area, work schedule, etc.).

3.8.2 NCOIC Review

3.8.2.1 Intent

The perceived intentions of this attribute are as follows:

- It extends the notion of role/identity/attribute-based access.

- This is not related to the producer/publisher (see Attribute 3: Information/Data Protection and Surety (Built-in Trust). The responsibility for trust is not incumbent on the information/ service producer[12].
- It can be used for, or extends to, agent proxies.
- Decoupling a device from service use from user's identity—A user invokes/uses a device (as an agent) to access a service. In the process, a user's identity is used, via the device, to gain authorization to access the service (e.g., access email via a smart phone).

3.8.2.2 Critique

This is an attribute more about, or an attribute of, the net-centric environment than it is of the individual systems and services that leverage and exist in that environment. What would the attribute of systems/services be that corresponds to this environment attribute and would allow determination of their degree of net-centric behavior? This aspect appears to be covered by Attribute 3: Information/Data Protection and Surety (Built-in Trust), which focuses on application services and systems taking responsibility for security, but leveraging environment services. The current attribute, Trusted and Tailored Access, is simply a more fine-grained representation of the factors that authentication and protection services might consider in making access permission decisions.

Additional issues include the following:

- "Trusted" and "tailored" are different concepts and require different technologies.
- "Technical capability" is unclear. Does it refer to a user's resource constraints? Does it include physical context (e.g., insecure area)? Perhaps "technical capability" should be seen as technical/environmental constraints (bandwidth, client device type, exposed area, etc.). More appropriate terminology for technical capability should be found.

3.8.3 NCOIC Recommendations

- This attribute, and attributes 2 and 9, could be categorized at the top level as infrastructure/ environment attributes that systems/services should demonstrate reliance on, rather than exhibit these attributes themselves, unless the program/project in question happens to be about infrastructure development or provisioning.
- This attribute should be combined with the next attribute, Attribute 9: Quality of Transport Service.

3.8.3.1 Candidate Replacement

See Section 3.9.3.1.

3.9 Attribute 9: Quality of Transport Service

Tailored for information form: voice, still imagery, video/moving imagery, data, and collaboration.

[12] However, the question of who is responsible for trust and trust by whom, or in what/who, must also be resolved—Is the network infrastructure provider or the provider of authentication services the one responsible for trust?

3.9.1 DoD Background

This attribute originally was titled Quality of Service (QoS). The term collaboration was included based on DoD user needs. It was realized that this attribute was only implicitly referring to transport services, not all of the different kinds of QoS that might be included. Transport was added to make the rest of the definition consistent with the title of the attribute. An alternative was to expand this attribute to include explicitly all other types of QoS (like quality of information, quality of operations, etc.), but such an expansion is difficult because these other types of QoS are difficult to obtain objective measures from the operational community.

3.9.2 NCOIC Review

3.9.2.1 Intent

The perceived intentions of this attribute are as follows:

- Recognize that not all bits are the same: Need to tailor transport to support different content priorities (e.g., streaming data vs. non-streaming) and/or different context priorities (e.g., under duress or not).

3.9.2.2 Critique

Tailored is not a quality measurement. It is not clear whether Tailored is quality or availability at some level of quality. QoS includes quality of operation service[13], quality of information service, and quality of transport service.

Collaboration is not a data form, hence seems out of place. Collaboration can create a data form; namely, a set of values for a state or representation of some portion of reality shared by the collaborators that is not necessarily yet shared (and may never be shared) with systems of record or users who are not part of the collaborating team. It could be viewed as a form of alternate reality shared by the collaborators.

This attribute overlaps greatly with Attribute 8: Trusted and Tailored Access. Both address tailoring in a related way. One addresses tailoring from a user's context and the other from a network context. However, the access to information transport related to a user's role, identity, or context is almost equivalent to the quality of transport to meet the user's needs, because those needs would be embedded in their role, identity, or context; otherwise, tailoring would not be possible (assuming the tailoring is derived from a user's role, identity, or context).

QoS should be dynamically negotiable supported by monitoring capabilities.

3.9.3 NCOIC Recommendations

Given the overlap and strong correlation between this attribute and Attribute 8: Trusted and Tailored Access, NCOIC recommends deleting reference to collaboration and combining these two attributes.

3.9.3.1 Candidate Replacement

The following candidate replacement attributes were arrived at after discussion of the original attribute. The important points of these discussions are listed in Sections 3.8.2.1, 3.8.2.2, 3.9.2.1, and 3.9.2.2. The candidate replacement attribute represents a more effective restatement of both the original

[13] Quality of Operation Service covers availability and reliability of services.

attributes 8 and 9 by focusing on the service level and its relation to the user and their context. NCOIC recommends that this attribute and attribute 8 be merged with the title and description changed to the following.

- **Tailored Resource Access**—Service levels can be modified, tailored, or negotiated to meet needs as represented by identities, roles, and/or contexts.

3.10 General Observations

A general observation is that the current set of DoD NCA is a flat conceptual space—the categories have no hierarchy. This flatness can become a problem if not all the attributes are intended to be used or applied in the same way or the same degree to every target program/project, system, or service.

Several attributes are represented in a fashion that focuses on the net-centric environment rather than on the NCA of the systems inhabiting that environment. NCOIC recommends that DoD consider a top-level structure for these attributes that then allows amplification of attributes in greater detail or domain-specificity for specific program/project types and attribute application contexts (discussed in greater detail in Section 5).

3.11 Missing Attributes

This section identifies areas that appear to be missing from the DoD NCA based on this NCOIC review.

3.11.1 Data Understandability

Many of the DoD NCA relate to the main net-centric design tenets of Data, Services, Information Assurance/Security, and Transport. However, DoD Directive 8320.02-G, under Data, addresses four key data design tenets for net-centric data sharing: data visibility, data accessibility, data understanding, and data trust. The current set of NCA does not specifically address data understanding.

Data understanding in a net-centric environment requires that data/information consumers can (1) discover what they need and (2) make use of the data for their purposes. These requirements necessarily entail the ability of the consumer to understand what is discoverable and understand the discovered data/information sufficiently to make use of it. Data understandability is realized in the terminology, vocabularies, and semantics used to discover and use data and information. Such understandability then entails the producer of data and information to be able to either anticipate their consumers and their contexts (i.e., vocabularies, terminology, and semantics) or provide mechanisms to mediate these differences.

3.11.1.1 NCOIC Recommendation

Though not properly represented in the original attributes, the NCOIC candidate replacement attributes of Post Data/Information for Network Access (Section 3.4.3.1), Information and Data Independence (Section 3.6.3.1), and Adaptive Information Access (Section 3.5.3.1) represent and realize the intent of data understandability and usability so no additional attribute is needed.

3.11.2 Human Interoperability

After this review was well underway, the following proposed attribute was added to the list of the original nine. This attribute is included to ensure that human-system integration is interoperable between the user population and the systems.

Attribute 10 Human Interoperability (HI)

Ensures human-system integration is interoperable between the user population and the systems for optimizing total human-system performance. HI addresses the human systems integration elements: human factors engineering and social system engineering factors for net-enabled operations/environments, and identifies the processes for integrating HI considerations across all system elements for adaptability and agility.

3.11.2.1 Intent

The perceived intentions of this attribute are as follows:

- The title suggests that the intent is to understand the "what" and "how" in building relational foundations to influence and/or anticipate behaviors of individuals, organizations, groups, societies, and cultures to establish compatible human networks that are reliable, effective, and trusted. As such, the attribute should account for any HI issues that may not be addressed in acquisition contexts. This would include policies, communication gaps, and the social information flow between disparate entities and groups; and social cues affecting the human individual and group willingness to share information regardless of cultural influences. Trust, as it is influenced by reputation, and other basic human instincts such as greed, fear, and power, will be critical to understanding this[14].
- The attribute also considers the impacts of social and cognitive integration. Programs/ projects and/or systems include measures of social and cognitive integration that facilitate their effective use. Such measures may apply to cognitive models of network users, dynamic exchange of social domain information among users, and/or formation of ad hoc social relationships among users in response to evolving mission/capability needs. Variables influencing integration might include, but are by no means complete, identity, attribution, affiliation (family, culture, institution, community of interest [COI], team), mood, demeanor, degree of understanding (cognitive matching), cognitive models, and social models.
- This is about human-to-human interactions mediated by technology (social system engineering)—as well as about human-to-system integration. The human-machine system, as technology evolves, will eventually act as an ecosystem where human and machine components will provide feedback and influence to each other.

3.11.2.2 Critique

Interoperability is both a technical and a socio-cultural phenomenon, and must be described in terms of the harmonization of people, processes, and technologies. As phrased, Attribute 10 is more of a definition than an attribute. It is principally about human-to-human interactions mediated by technology (social system engineering)—as well as about human-to-system integration. The human-machine system,

[14] Adapted from National Defense University Human Interoperability Enterprise Working Group Definition, 2009. Activity sponsored by Office of the Secretary of Defense for Networks and Information Integration.

as technology evolves, eventually will act as an ecosystem where human and machine components will provide feedback and influence to each other.

The ability to qualify or quantify this is complicated and in most cases difficult to validate. It also appears to be closely associated with or overlaps the missing non-technological attributes discussed in Section 3.11.3, but highlights a particular non-technological attribute without making it clear why this attribute is being singled out from the other possible non-technological attributes.

NCOIC agrees that HI is an important aspect of NCO and behavior. It requires explicit representations of cognitive models and social cues used in the system or assumed in expected behaviors, as well as a means for systems to use these in their (run time) interactions with network users. These representations can be a means for users to discover and use information and services, to facilitate interaction with each other, and support systems in pursuit of operational objectives.

3.11.2.3 NCOIC Recommendations

The phrasing and description of the proposed attribute should make it clear how it differs from other non-technological attributes that might be important from a net-centric interoperability perspective. The attribute should be phrased so that it is clearly distinguishable from traditional human-system integration, often viewed as a specialty engineering discipline within system engineering. NCOIC recommends that a restatement of the attribute title and description be considered.

The following is a prototype candidate replacement and requires further follow-on work:

- **Social and Cognitive Integration**—Programs/projects and/or systems include measures of social and cognitive integration that facilitate their effective use. Such measures may apply to cognitive models of network users, dynamic exchange of social domain information among users, and/or formation of ad hoc social relationships among users in response to evolving mission/capability needs. Variables influencing integration might include, but is by no means complete, identity, attribution, affiliation (family, culture, institution, COI, team), mood demeanor, degree of understanding (cognitive matching), cognitive models, and social models.

3.11.3 Non-technological Attributes

In addition to technological attributes, net-centric attributes also should address non-technological areas that impact net-centric operations. These additional areas would be useful to developers, architects, program mangers, and the acquisition community in enhancing existing systems as well as developing new systems that meet their needs for information sharing and interoperability. Creating separate sets of attributes for non-technological attributes must take into consideration relationships between these and their impact on technical attributes. The difficulty in creating such attributes and their associated relationships is the overlap they have with each other and distinguishing this overlap with sufficient precision to make the attributes useful and effective.

Obstacles to interoperability, such as multiplicity of perspectives, semantic conflicts, contextual conflicts, organizational and acquisition models, could be mitigated by addressing these non-technological areas, as well as the transformational aspects described (see Section 6.2). However, having attributes in these non-technological areas may help projects achieve their net-centric and interoperability goals.

3.11.3.1 Non-technological Areas

Non-technological areas include the following:

- Policy
- Operational
- Organizational
- Cultural
- Business Model

3.11.3.1.1 Policy

Organizations establish policies that impact technological aspects of systems and can constrain how efficiently NCO can be conducted (e.g., IA policies). Or, viewed conversely, these policies can enable NCO to be conducted more effectively (or at all) in a given context by ensuring that information is protected adequately and provided when needed. Such policies can impact issues of trust, IA, and QoS, in addition to the overall business model and procurement practices (e.g., Net-Ready Key Performance Parameters). The attributes for this area need to qualify or quantify those policies that impact technical aspects of systems.

3.11.3.1.2 Operational

A general issue in net-centric environments concerns the lack of knowledge of additional systems in the environment as a particular system is in development: Knowledge of the net-centric environment into which the system being developed will exist. That risk, dependency management, raises indemnification issues for a system incorporating some service or capability based on the existence of some other system's service that has not yet been deployed.

The NCOIC SCOPE™ model points out that operational/functional and organizational scope issues are manifested in the data models and service interfaces of the various systems that contribute to any given capability. The more operational scope a given service can handle, the easier it is to use by someone else on the network—the one-stop shopping principle at work. On the other hand, if there are many different services, each with its own and different operational and organizational scope, the user on the network must have a much greater operational domain knowledge to compose the multiple service requests that might then be needed to address a particular information or service requirement for some capability.

To illustrate the point of operational scope, take the case of the used car buying service CarMax. It is accessible over the Internet and only sells used cars and only in the United States (and not in all states). But it sells all makes and models of cars, but not trucks over a certain size or golf carts or farm vehicles. It does not sell new Nissan or General Motors vehicles. By contrast, the equivalent Nissan site sells only new Nissans and the General Motors site sells only new General Motors cars. There are, however, new car buying services, such as the one offered by United Services Automobile Association (USAA), that allow a person to shop for a new car from any of the major manufacturers. Each of these net-centric services represents a different set of operational scope tradeoffs that appeal to different customer communities who have made different car purchase strategy decisions. In the case of the new car buying service approach, the search requests to the different new car manufacturers still take place, but the complexity of finding and invoking the appropriate manufacturer-specific services is hidden from the

user, and they provide additional value to the shopper by providing greater price visibility and discounts than the individual manufacturer sites or dealer sites offer.

Any one-stop shopping convenience has to be balanced by the fact that some decomposition into services with different operational/functional and organizational scope will always exist, so it is important that whatever services might be offered by some system, the scope of such services be advertised explicitly. This allows both the various individual users of such services and the value-added aggregators/resellers to understand properly what the service is providing and what it is not, and to make appropriate decisions about what other services they might want or need to access in order to achieve their operational objectives. A key nontechnical net-centric attribute then, is the degree of explicitness and comprehensiveness with which a system or program/project advertises its scope.

3.11.3.1.3 Organizational

NCO necessarily requires sharing among, and dependencies on, different organizations. Systems to be used in, or developed for, the net-centric environment need to address explicitly these sharing and dependency issues. The overall constraints to these issues usually derive from organizational culture and policies. For example, decisions to outsource certain institutional functions, such as help desk services, manufacturing services, or warehousing/distribution services, rarely are made on purely economic grounds. Sending jobs overseas or even just to another state or jurisdiction is not something done without considering corporate culture, the risks of dependency on organizations outside one's direct control, and regional politics. Which institutional positions can see what information and request/execute which services likewise are driven by organizational culture and policies. In defense or government organizations, different information security domains and labeling/tagging conventions often are aligned with organizational boundaries.

A related point is that in system/capability acquisition today. The scope of the respective systems/capabilities is defined in the organizational/administrative domain and there is no real institutional framework or corresponding system for managing the scope relationships among the many systems/capabilities in development or in operational use. This makes it difficult to realize the intent of many of the other NCA because discovery and binding to other capability fragments on the network is done bottom-up and opportunistically, with significant risk of overlapping services or missing resources that exist, but which the seeker does not discover. The recent Portfolio Management initiative in the US DoD is an attempt to address some aspects of this problem, as is encouragement of the formation of COIs. However, these remain fragmentary solutions to the problem.

Attributes in the area of organizational scope need to qualify the organizational policies and overall culture related to sharing and the risk they are willing to assume to allow sharing of information and services with other organizations over a network and be dependent on the services of other organizations, real or virtual (e.g., COI). These attributes also need to address the degree to which organizations demonstrate their stated policies with commensurate resource allocations and incentive structures for open, net-centric behaviors.

3.11.3.1.4 Cultural

An organization reflects both the larger culture in which it exists and its own internal culture. The culture may or may not be policy driven or encourage creativity. In each case, the culture will have an impact on an organization's approach to decision making and hence, to its business model and acquisition processes. Attributes in the cultural area need to qualify the impact of the culture on technological and operational aspects.

3.11.3.1.5 Business Model

The business models currently employed can be impediments to achieving net-centricity. They do not provide adequate, if any, incentives for programs/projects to perform the net-centric behavior of exploring their network environment and identifying the possible capabilities or services that could be used to implement their program/project requirements and accept the attendant interdependency and scope risks.

3.11.3.1.6 Summary

As can be seen from the brief discussion of each of these non-technological attribute areas, there are many factors that can impact or characterize net-centric behavior that have nothing to do with technology. Although net-centric technology might enable, facilitate, or inhibit the range of attribute values, someone might be willing to accommodate in some of these attribute areas. It should also be clear from these brief discussions that the number of possible non-technological attributes relevant to DoD's purposes for developing the NCA would require a much more extensive exposition than is appropriate for this invited review. However, NCOIC already has developed an extensive set of non-technological NCA in its SCOPE™ model that address these attribute areas to a considerable degree.

3.11.3.2 NCOIC Recommendations

NCOIC recommends that DoD consider adding NCA in the non-technological areas to be developed based on the relevant SCOPE™ dimensions, augmenting them where needed, and updating the SCOPE™ model with these changes. In particular, NCOIC recommends adding a NCA that raises programmatic consciousness with regard to the issue of program/project scope and its relationship to other programs/projects and capabilities in operational scope space. The following are possible starting points:

- The program/project has defined its operational scope with respect to accepted measures of such scope and identified points of intersection and dependencies with related capabilities and their operational scope.

- The program/project has engaged appropriate COI to address the understandability and operational scope and terminology issues associated with interacting with these adjacent domains.

3.12 NCOIC Candidate Net-Centric Attributes Summary

There are 10 candidate replacement attributes recommended by the NCOIC. These replacement attributes are summarized in Table 3.

Table 3. NCOIC Candidate NCA Summary

Title	Description
Media Independence	Information used, produced, published, or disseminated by the services or systems is decoupled from transport mechanisms.
Open-Ended Pervasive Accessibility	Ability of system(s) or services(s) to find, use, and control information (which requires an ability to identify and distinguish entities and the publication of information with minimal a priori constraints).
Open Standards Based	To support interoperability programs/projects, systems, and services must maximize the use of openly available and unencumbered technical and process standards that support media independence, pervasive accessibility, and trustworthy control of access to information and services.
Protected and Assured Transport Services	Program/project, system, or service makes use of existing specified assurance, protected, and defended transport services where feasible/available. Infrastructure systems provide specified assurance, protected, and defended transport services that are accessible and available wherever and whenever needed.
Producer/Publisher Trust Relationships(with users and services)	Program, system, and/or service(s) have mechanisms for establishing and maintaining appropriate trust relationships with users and services on the network. Measures are taken to comply with any security labeling, data protection, and access control requirements entailed by the trust relationships and monitor the environment to ensure that conditions on which the trust relationships were established have not changed.
Post Data/Information for Network Access	Program/project, system, and/or service(s) have made their products discoverable and accessible on the network in a manner and timeframe appropriate to the nature of the information/data.
Adaptive Information Access	Program/project, system, and/or service(s) has provided users and services access to information and data in ways most appropriate for their context while allowing them to negotiate access arrangements and understand the associated costs.
Information and Data Independence	Program/project and/or system has separated its information and data from applications and services (dependencies) and is provided with sufficient context (i.e., metadata) to enable users to use the information/data correctly for their purposes.
Tailored Resource Access	Service levels can be modified, tailored, or negotiated to meet needs as represented by identities, roles, and/or contexts.
Social and Cognitive Integration	Programs/projects and/or systems include measures of social and cognitive integration that facilitate their effective use.

4 Development of Core Net-Centric Attributes

4.1 Abstraction to Minimum Common Level—Principles

The NCOIC Execution Plan calls for the consistent development of attributes that can be described in terms that minimize ambiguity and are responsive to net-centric environment drivers. This suggests the need to identify and define a set of axioms or principles from which the attributes may be derived. These axioms or principles would represent those aspects that are independent of context and that are less subject to change, and consequently, are more abstract.

The process to define a set of principles from which NCA can be derived involves abstraction to a common level (i.e., abductive reasoning) and includes the areas considered missing as described in Section 3.11. The minimum common set should address all areas considered necessary for net-centricity as represented in the SCOPE™ model[15].

To meet the goal of a minimal set of common principles and related attributes, it must be understood what an attribute is and its relationship to other concepts. For this review, and as part of the NCOIC Lexicon, the following definition is adopted:

- Attribute—A feature, or characteristic whereby objects or individuals can be distinguished and that admits qualification or quantification.

It is the NCOIC position that attributes are derivative of more fundamental concepts or principles. Again, for this review, and as part of the NCOIC Lexicon, the following definition is adopted:

- Principle—A basic context-independent generalization that is accepted as true and that can be used as a basis for reasoning or conduct.

Simply put, principles allow the selection[16] of attributes that are deemed useful to distinguish or select systems, programs, or projects. Thus, core principles of net-centricity are a minimal set that can be used to distinguish essential and relevant attributes of net-centricity, providing the basis for consistent evolution of attributes.

4.1.1 NCOIC Core Net-Centric Principles

Table 4 is a short list of the (current) principles. A more complete description can be found in the NCOIC paper, *Net-Centric Principles*[17]. These principles are not necessarily disjoint/independent nor prioritized, though in practice, the principle of *Pragmatism* can trump other principles.

[15] https://www.ncoic.org/apps/group_public/download.php/8504/SCOPE_MODEL_VER1.0.pdf
[16] The notion of principle is used in a more constrained fashion with the intent of an interpretation more closely aligned with that of axiom from formal reasoning systems (with the attendant ability to derive consequences from these axioms).
[17] Note, at the time of writing this paper is still in draft and has not yet been formally accepted as an NCOIC product.

Table 4. NCOIC Core Net-Centric Principles

	Title	Description
1	Explicitness	An entity should make all information about itself explicit.
2	Symmetry/Reciprocal Behaviors	Relations and entities should exhibit symmetric characteristics and behaviors.
3	Dynamism	Entities should support dynamic behaviors.
4	Globalism	There should be no a priori bounds on the scope on applicability.
5	Omnipresent/Ubiquitous Accessibility	Entities should have omnipresent or ubiquitous access to resources.
6	Entity Primacy	Entities have existence distinct from the contexts in which they participate.
7	Relationship Management	Relations should be explicitly represented and provide for negotiation, creation, change, and termination.
8	Open World	There is incomplete knowledge of the operational environment.
9	Pragmatism	The ability to improve operational effectiveness is paramount.

4.1.2 Mapping Core Net-Centric Principles to Recommended Net-Centric Attributes

Table 5 provides the mapping of the NCOIC principles to the candidate NCA. A complete description of how an attribute realizes, or is mapped from a principle (i.e., derived[18] from a principle), will be developed in a future NCOIC paper (see Section 7).

Table 5 represents an exercise in consistency and completeness: No NCA have been identified that cannot be mapped to one or more net-centric principles and there are no (current) net-centric principles that are not associated with at least one attribute.

Table 5. Principles to Attributes Mapping

Principle(s)	Attribute Title	Attribute Description
• Entity Primacy • Globalism • Omnipresent/Ubiquitous Accessibility • Pragmatism	Media Independence	Information used, produced, published, or disseminated by the services or systems is decoupled from transport mechanisms.
• Globalism • Omnipresent/Ubiquitous Accessibility • Pragmatism	Open-Ended Pervasive Accessibility	The system(s) or service(s) has the ability to find, use, and control information (which requires an ability to identify and distinguish entities and the publication of information with minimal a

[18] A simple notion of derived is that of modal necessity. An attribute A is derivable from principle P, if any realization of A necessarily realizes P.

• Open World		priori constraints).
• Entity Primacy • Relationship Management • Symmetry/Reciprocal Behaviors	Protected and Assured Transport Services	The program/project, system, or service makes use of existing specified assurance, protected, and defended transport services where feasible/ available. The infrastructure systems provide specified assurance, protected, and defended transport services that are accessible and available wherever and whenever needed.
• Relationship Management • Explicitness • Entity Primacy • Dynamism • Open World	Producer/Publisher Trust Relationships(with users and services)	The program/project, system, and/or service(s) have mechanisms for establishing and maintaining appropriate trust relationships with users and services on the network. Measures are taken to comply with any security labeling, data protection, and access control requirements entailed by the trust relationships and monitor the environment to ensure that conditions on which the trust relationships were established have not changed.
• Omnipresent/Ubiquitous Accessibility • Dynamism • Explicitness	Post Data/Information for Network Access	The program, system, and/or service(s) have made their products discoverable and accessible on the network in a manner and timeframe appropriate to the nature of the information/data.
• Relationship Management • Pragmatism • Symmetry/Reciprocal Behaviors	Adaptive Information Access	The program/project, system, and/or service(s) has provided users and services access to information and data in ways most appropriate for their context while allowing them to negotiate access arrangements and understand the associated costs.
• Dynamism • Explicitness • Symmetry/Reciprocal Behaviors	Information and Data Independence	The program/project and/or system has separated its information and data from applications and services (dependencies) and is provided with sufficient context (i.e., metadata) to enable users to use the information/ data correctly for their purposes.
• Relationship Management • Omnipresent/Ubiquitous Accessibility	Tailored Resource Access	Service levels can be modified, tailored, or negotiated to meet needs as represented by identities, roles, and/or contexts.

5 Assessment Contexts

The term assessment context is used to describe constraints on the interpretation of the NCA or their values based on the contexts in which the NCA, or their derivatives/variants, may be used. The key reason for exploring assessment contexts is that the NCA are not equally applicable nor equally important in all possible contexts. For example, a legal assessment of a security breach may be different from a technical assessment of the same security breach. The use of the NCA may not be an evaluation in a formal sense (e.g., a result provided to a customer or upper management), and it may be tied to, or driven by, various events that might occur in an enterprise or system life cycle or on a program. Indeed, some attributes may not be applicable at all in some contexts. For example, use of the assured services attribute may not apply to open source information services to the same degree or be assessed in the same way as it would be for a highly sensitive and critical national security service. Or the attributes may require different degrees of specificity to be useful in some contexts. For example, an NCA that is more than adequately specified to ensure that an emerging operational capability concept is suitably net-centric may be hopelessly vague when applied to assessing the net-centricity of a particular embedded system software design, and vice versa. The DoD NCA recognize some differences in assessment contexts with the inclusion of the functional entities to describe different stakeholder types (i.e., assessment contexts) in the DoD net-centric ecosystem.

But there are assessment context attributes besides DoD stakeholder types. NCOIC believes it is useful to consider four major assessment context dimensions that drive selection of NCA and attribute value ranges, as well as analysis or evaluation methods:

1. Enterprise Context
2. Life Cycle Phase (of system/capability being assessed)
3. Type of System/Capability
4. Attribute Application Purpose

5.1 Enterprise Context

The first assessment context dimension, Enterprise Context, is frequently overlooked because most programs and enterprises take their enterprise context as a given. But since net-centricity transcends enterprises, it is important to be explicit about the enterprise context in which a given application of NCA is taking place. Since the purpose of net-centricity is greater operational effectiveness through better use of what resources an enterprise has available to it, including those of other enterprises, the specific desirability or importance of the various possible NCA will vary from one enterprise to another.

So the specific NCA important to the US DoD and the particular [attribute] values desirable for particular attributes are likely to be different for NATO, the US Department of Homeland Security (DHS), or a commercial firm such as Hewlett Packard or Proctor and Gamble in their supply chain operations.

Any application of NCA should therefore start by explicitly establishing the enterprise context to be used for the application or evaluation. This context will drive selection of the top-level set of NCA to be considered for the evaluation, such as the US DoD NCA reviewed in this document. An initial review of the NCOIC SCOPE™ model dimensions for enterprise/capability scope can help establish enterprise context attributes and values that may drive selection of more detailed/specific attributes for the

evaluation, such as enterprise breadth attributes, security policy attributes, and domain-dependent attributes.

5.2 Life Cycle Phase

The second assessment context, Life Cycle Phase, tends to be given less attention than it deserves, in part because the system/capability acquisition process focuses on acquisition as a one-time event or process, with the thing being acquired continuing to exist statically for the remainder of its useful life after the acquisition is completed. But a key principle and driver of net-centricity is dynamism and the NCA that were appropriate last year may not be the most appropriate or valued the same this year or in some future year. So it may be perfectly reasonable to perform a net-centric evaluation of a system after it is deployed operationally, possibly more than once. The focus of evaluations will continue to be the acquisition phases of the system life cycle. But the attributes that are important to look at early in the development of a capability may be a fait accompli later in the development of that capability. As a system progresses through design, integration, and test, the attributes that become important to look at take on a more design/implementation-specific characteristic. These attributes need to be more measurable/ quantitative and testable as the system nears operational readiness.

What the above possibilities suggest is that several different decompositions/refinements of the DoD NCA need to be developed that can be applied in the requirements exploration/validation phase (e.g., early in JCIDS), the high-level architecture/design definition phase, the detailed design phase, and the integration/test phase of systems/capabilities. The attributes will become increasingly technical and specific to design and implementation elements over this progression, such as use of specific enterprise services and compliance with specific cyber security technical standards and components/services.

5.3 System/Capability Type

The third assessment context, Type of System/Capability, is already captured to some degree in the Functional Entities concept employed in the current DoD NCA guidance. For example, a communications/network infrastructure provider has a different perspective on essential elements of information and information sharing than the developer of a sensor system at the tactical edge of the network, or the user of a command and control application that leverages both the communications infrastructure and a multitude of different sensor systems. These perspectives reflect the assessment contexts of the information transport service provider, the information producer, and the user/consumer functional entities in the DoD NCA guidance, respectively. For example, applying the Media Independence attribute to a transport service provider may make little sense if the transport protocols and services have very media-specific attributes (e.g., SATCOM, fiber-optic, wireless). The sensor system may be constrained to use wireless connections and may have very limited bandwidth and storage capacity, making assessments using the Media Independence and Post in Parallel NCA problematic without significant tailoring. Likewise, the user of command and control applications may have little insight into or concern about the Quality of Transport Services NCA other than the fact that those services need to be there in the background. Assessing such applications using the Quality of Transport Services NCA would require a significantly different representation of that attribute than would assessment of an information transport service.

Essentially, this assessment context dimension looks at the nature of a system/capability and what that might imply or entail regarding the degree to which net-centricity may facilitate their operational utility or the degree to which their environment may constrain net-centricity. In NCOIC SCOPE™ model terms, there are systems/capabilities that are characterized by the less feasible value ranges on the

technical/economic feasibility dimensions. An example might be systems that operate in a disadvantaged networking environment, or systems that need to operate internationally. So this assessment context dimension needs to combine the Functional Entities decomposition with additional program-type attributes (e.g., tactical system vice garrison or "back office" system) to provide guidance for selection of appropriate NCA for program types that exhibit these attributes/value ranges.

5.4 Attribute Application Purpose

The fourth assessment context dimension that needs to be considered is that of purpose, why are the NCA being applied?. Helping operational analysts to think more net-centrically about a possible operational capability requires a different set of NCA and a different mode of use than trying to score a specific capability or system against established enterprise net-centric standards for compliance. There are two important purpose contexts. In the first, the purpose attribute should be provocative and cause the user of the attribute to examine the many implicit assumptions everyone tends to make (i.e., promote "out-of-the-box" thinking). The wording of the attribute should be fairly "open-ended" and not very specific or detail oriented. On the other hand, the set of attributes considered should be as comprehensive and inclusive as possible, lest some aspect of the "box" be overlooked in thinking about the potential capability. By contrast, in the second purpose context, the attribute should be as specific and measurable as possible, and attributes that aren't clearly relevant to determining compliance should not be examined lest the evaluator's time be wasted with useless or unanswerable questions. Another attribute assessment purpose might be to help determine funding decisions for a portfolio of possible systems or capabilities competing to be selected for implementation. NCA for such a purpose would be at a level of specificity and comprehensiveness intermediate between the two purpose context extremes just discussed.

Purpose was one of the challenges faced by NCOIC in combining/merging the NCAT™ tool and attributes with the SCOPE™ model dimensions. The former were aimed at scoring and weighting a specific design or architecture against a specific set of compliance criteria, while the latter was aimed at exploring NCA space for new capabilities and services. There is a correlation between the purpose assessment context dimension and the life-cycle phase assessment context dimension, but they represent distinct concerns. For example, an organization may want to explore how a legacy system could be modified to become more net-centric for certain operational purposes or to reduce operational or support costs by making use of newly emerging capabilities on the network. A scoring/compliance purpose would not be appropriate in such an assessment context, but would be appropriate once a decision is made to implement specific net-centric changes in the legacy system and the sponsor wants to check progress toward implanting the technical changes necessary to achieve the target level of net-centricity.

5.5 Assessment Context Summary

In summary, an assessment context modifies either the interpretation of an NCA or the range of possible answers that may be expected for that context. The four assessment contexts described above drive both the selection of the NCA and attribute values that might be important and appropriate for a given assessment context. They also guide the selection of the appropriate evaluation or analysis method. For example, a net-centric requirements exploration workshop might be appropriate to be used by a COI developing domain concepts and standards for services and data exchange across multiple organizations/systems. A compliance evaluation might be done by having multiple assessors use the NCAT™ tool and examining design artifacts for evidence of specific attribute values to be selected for each NCAT™ question. A future NCOIC paper will address the specifics of describing assessment

contexts and developing the procedures and guidance for tailoring and applying the attributes in these diverse assessment contexts.

6 Net-Centric Attributes Management

The nature of net-centricity suggests that the NCA identified by DoD or NCOIC will evolve over time. NCA evolution is driven by changes in the operational and technical environments, more capable network and information infrastructures. In addition, changes in both the established base of existing programs/systems and in perspectives of such programs regarding the desirability of working in a more net-centric fashion with other programs/systems and the organizations they represent will drive the evolution of NCA. The attributes and their derivatives or specializations are likely to evolve to support different assessment contexts, ranging from capability concept development, to portfolio management, to operational testing of a deployed system or service.

NCOIC has attempted to provide a basis for an understanding, organization, and hence, the management of the evolution of NCA by the development of core net-centric principles. The principles have been developed with the presumption that the attributes needed to develop net-centric programs and systems can be derived from them. Their original development was in response to this review of the DoD NCA.

6.1 Key Drivers for Attribute Evolution

The key drivers for evolution of the NCA are as follows:

- Relevance—Degree to which manifestation of the attributes results in changes in system and program behavior that improves their ability to interoperate and support more dynamic and agile operational contexts.
- Ease and simplicity of application of the attributes, including the objectivity and quantitative nature of the measurements.
- Appropriateness of the attributes to the assessment context and scope.
- Availability and cost of enabling network technology, infrastructure, and services.
- Improved net-centric characteristics of the installed base of systems.
- Increased awareness and willingness of people and organizations to work with each other and depend on each other.
- Changes in the acquisition model that incentivize this kind of behavior.
- Development of guidelines for balancing the risks, costs, and constraints of net-centric behavior against the benefits that might accrue from such behavior, depending on operational context.

Each of these drivers for evolution are discussed regarding their rationale and potential influence on the evolution of NCA.

6.1.1 Relevance

Relevance is probably the biggest driver of evolution. The ultimate utility of the attributes is determined by their ability to predict or influence the resulting operational utility, adaptability, or agility of the systems and capabilities to which they are applied through characterization or evaluation.

Measures of operational effectiveness are diverse and vary greatly across different capability types. Thus, NCA are likely to become more specific to certain operational domains or COIs. This specialization will entail that their operational relevance is more readily apparent to the capability/program stakeholders.

6.1.2 Application Simplicity

Closely related to [attribute] relevance is the drive for simplicity in applying or measuring the attributes. If the attribute is hard to measure or describe quantitatively and objectively or repeatedly, it will have limited utility in influencing the direction that systems and programs take. The need for simple applicability tends to evolve the attributes from broad statements of desirable characteristics to more specific, measurable quantities or properties of systems. The challenge is, and will continue to be, to keep proliferation of attributes in check and to make it clear and easy to decide which measurable attributes are appropriate to some arbitrary system or capability. The other challenge is to be wary of using measurable attributes because they are easily measurable rather than attributes that are actually good predictors of operational utility/effectiveness.

6.1.3 Appropriateness

Appropriateness to the assessment/employment context is another important driver of attribute evolution. Attributes that are appropriate for characterizing a capability concept are not equally appropriate to measuring a system going through operational testing. The NCA are likely to evolve for appropriateness and utility during the capability requirements development process and to support portfolio management processes, while a related set of attributes will evolve to better support the system development, testing, and assessment contexts.

6.1.4 Availability

Increasing availability and declining cost of networking technologies and infrastructure services will change the tradeoffs among NCA related to technical and economic feasibility of NCO. Improvements in network security, assurance, and QoS technologies will reduce the barriers to net-centric behavior. At the same time, these improvements will enable novel business models for enabling net-centric behavior and across a wider range of operational domains than is generally feasible today. New NCA related to more dynamic business models for accessing network and mission services are likely to come into being and evolve. For example, explicit representation of the business model for accessing certain net-centric services might become an NCA in the not too distant future, especially if the service is not provided organically by the DoD.

6.1.5 Net-Centric Base

Today, systems under development tend to view themselves as pioneers in introducing NCA into the DoD system environment, with most of the systems already deployed exhibiting largely legacy system behavior, and not willing or motivated to change their existing interfaces. As the base of deployed systems incorporate an increasing percentage of capabilities with significant NCA values, the willingness of systems to rely on each other's services will increase. This increased reliance engenders the types and levels of NCA, both expected of others and willing to be provided by system sponsors, to increase. More specific NCA are likely to arise, especially those relevant to or driven by a specific COI or portfolio of programs.

6.1.6 Organizational and Cultural Change

Over time, the pressure for more joint and coalition operations and operating behavior and greater operational agility will result in cultural changes that make organizations more willing to engage in net-centric behavior with each other, including increasing interdependence. These dependencies will drive more explicit recognition of the interdependence among programs and systems. In turn, this forces establishment of budgetary processes, management, and business model changes that facilitate net-centric behavior. NCA that focus on these aspects of organizational behavior are likely to arise and be incorporated into the net-centric lexicon and landscape.

6.1.7 Acquisition Models

Changes in the acquisition model for systems that reward more open interfaces and responsive behavior on the part of program managers and system sponsors suggest that some NCA will be developed to guide, measure, and characterize systems and services from the acquisition model perspective. For example, one desirable attribute for net-centric systems from an acquisition perspective is the degree to which the system captures information about use of its services by other systems, or what development costs were avoided by leveraging existing system capabilities accessible over the network.

6.1.8 Balancing Risks, Costs, and Constraints

Currently, the DoD NCA are focused on attributes that are desirable from a net-centric perspective, but do not include any attributes that represent the costs or constraints introduced by net-centric behavior and interdependence. As a consequence, this focus creates a bit of an adversarial relationship between the program managers and the DoD organizations responsible for net-centric advocacy and enablement. There is no inherent counterweight to improving any and all NCA of a given system—there is no good-enough solution to how much net-centric behavior is appropriate for a given system or capability. Some attributes are therefore needed that reflect the cost and technical feasibility of net-centricity for a given system or capability context so that reasonable tradeoffs can be made. Explicit guidance for making such tradeoffs should be part of any NCA program within DoD. Problem space attributes that mitigate against increased net-centricity should become part of the attribute set, thereby allowing the process stability that can be achieved only by negative feedback loops. Otherwise, NCA become inherently open-ended and essentially unsatisfiable requirements.

6.2 Transformational Approach

The transformational aspect of net-centricity and interoperability needs to be considered in the attributes. Of necessity, most systems will migrate from existing or legacy technologies rather than being reinvented as new development. Thus, transformation is a pre-implementation phase that is defined here as the migration of an existing or legacy system from their current state of operations to a future state of needed net-centricity. Giving consideration to transformation in the attributes emphasizes the need for architects to capture the existing or legacy enterprise (or domain, COI, family of systems, etc.) artifacts and can assist them in better preparing an enterprise (or domain, COI, family of systems, etc.) for transitioning to net-centricity. Having formal, repeatable, and consistent (standards-based) tools and approaches for capturing (and managing) this information can be a key driver for incremental migration for legacy systems.

Some of the attribute drivers described above in Section 6.1 have been presented mostly in the context of the US DoD. Net-centric behavior does not end at the boundary of the US DoD, nor at the boundary of

the United States, nor at the boundary between federal government and local governments, nor with commercial enterprises, nor with private citizens—net-centricity is a cross-boundary behavior.

There are numerous business model innovations underway as a result of net-centric enabling technology and infrastructure (e.g., cloud computing, virtual worlds, and social networks), and complementary socio-political transformations are occurring as a consequence of these business model innovations. A key net-centric enabler here is the issue of identity and the dynamic coupling of identity to institutional frames of reference – in contrast to past static contexts for identities. The issue of identity is one reason for introducing the notion of Entity Primacy as a key net-centric principle to distinguish net-centric behavior from past Primacy of the Collective approaches to characterizing systems, networks, and user identities (e.g., system user ID).

A related transformational NCA area is that of degree of indirection among systems and the institutional entities they represent. Past non-net-centric approaches tend to view system interfaces as being directly coupled with other specific systems. This does not imply that third-party interactions do not occur, but they tend to be (viewed as) hidden behind the direct interfaces that system A has with system B. The net-centric transformation makes it easier to create business models and new systems whose primary role is aggregating and translating information from other systems rather than originating this information. Such capabilities puts a premium on managing the provenance of information and any restrictions or rights that might be associated with the information obtained from third-party systems. NCA that measure or characterize systems or services from the perspective of how well or how broadly systems might manage information obtained from others might be needed to support and facilitate this kind of transformational behavior, both inside DoD and with outside organizations.

6.3 Evolution of Net-Centric Attributes – NATO Network Enabled Capability (NNEC), US Department of Homeland Security, Commercial Industry

While the DoD NCA evolve as a result of the drivers described in Section 6.1, similar pressures will push other organizations to evolve their conceptual models of net-centric behavior as well, albeit with somewhat different priorities and areas of focus.

NNEC[19] will evolve based on the challenges of a large multinational alliance attempting to expand its operational mission areas and deal with the unique relationship it has with the European Union, which has launched a number of net-centric initiatives in the defense, air traffic control, and electronic, participatory, government areas. Similar considerations will drive the evolution of NCA for other nations as well, especially those that have significant business and government interactions with NATO and the European Union. International air traffic control/management, international travel, and international commerce/customs are likely to be early focus areas for this evolution.

The US DHS faces challenges in becoming more net-centric within and among the many legacy agencies that it comprises, as well as with local and state governments, commercial entities, and with other US federal departments and agencies and external governments. Privacy, civil liberties, and law enforcement aspects of NCA will play a prominent role in their evolution within the US DHS. Partnership with DoD and the US Intelligence community will help drive co-evolution of the NCA for this particular COI.

[19] https://transnet.act.nato.int/WISE/Informatio

Commercial industry obviously is not immune from evolutionary pressures regarding what constitutes net-centric behavior. Globalization, "eBusiness" potential, and competition are big drivers for commerce. Supply chains for modern business are usually global in nature, as are the markets for the resulting products and services. Even the enabling infrastructure services and execution platforms are becoming more net-centric—the key factor behind the advent of cloud computing. Global gaming networks, virtual worlds, smart phones, and social networks are raising expectations among consumers regarding who they can interact with and about what, and for what reasons, across the globe. Indeed, this evolution has created a new social reality that previously was inconceivable, much less as realizable as it already is today.

6.4 Environment, Functional Entity, or Assessment Context

The net-centric environment creates an ecosystem in which functional entities interact with each other at various stages of their life cycle and in varying application/operational contexts (thus evolving the net-centric environment). Until now, NCA have focused on system development and a small set of assessment contexts. These contexts will not go away, but will be augmented with additional NCA assessment contexts. Some of these assessment contexts may refine (i.e., be subcontexts of) those identified in Section 5. For instance, organizational acquisition and divestiture may be considered subcontexts of an overall Enterprise context. Reengineering could be a subcontext of the Systems/Capability Type context. Other contexts might be open or transparent government initiatives. And others might be social network or other more peer-to-peer oriented endeavors for which there is no strong central authority and very limited or no legal recourse.

From an NCOIC and DoD perspective, the following assessment contexts are likely to be the most operative:

1. System or capability concept development or enterprise integration/reengineering—How net-centric should/could this system, capability, or enterprise be? What should the business model for the capability be? This is an example of both an Enterprise and a Systems/Capability assessment context types.
2. Portfolio or product line (family of systems) management—How should functionality be decomposed, parameterized, and shared among systems/products in the portfolio or product line? This also supports budgeting process and allocation of budgets across a portfolio or product line. This is an example of an Enterprise assessment context type.
3. System/system-of-systems architecture and design evaluation—How net-centric is the system design or architecture (as is or to be)? This is an example of a Systems/Capability assessment context type.
4. Pattern characterization for operational, capability, and technical contexts—What is the operational and institutional scope of the pattern and how net-centric is it? A subsidiary context is at the building block level—how well and to what degree does the building block comply with the guidance in the pattern(s) that it is a part of? This is an example of an Enterprise assessment context type.
5. System/service deployment—How net-centric is the implementation of the design for some system or service in the target operational network environment (including any explicit scope assumptions for the system or service)? This is an example of a Systems/Capability assessment context type.

There may be additional significant assessment contexts, and there is some overlap between the assessment context types identified here. However, these assessment context types are likely to be the ones encountered most frequently by NCOIC member companies and customers, and they are different enough to result in at least some unique attribute types or possible attribute values for each context type. NCA should be characterized as to their suitability for each of these context types, or simply labeled as to the context type that is their primary target. Additionally, the institutional and/or operational domain scope of the attribute should be associated with the attribute so that it can be identified appropriately and selected in a given NCA application context.

6.5 Infrastructure and Processes to Support Evolution of NCA

Continuous and dynamic feedback in support of NCA evolution is sought. In this way, the current review effort can transition from a static one-time review to a dynamic process by which the NCA are kept current, benefiting both government and industry. This also supports an industry evolution plan.

Under the work of its Building Blocks Team, NCOIC is using the following design structure to organize, describe, and make available NCOIC data:

- Pattern Repository—A metadata extract of key information about NCOIC deliverables.
- Open Standards Registry—A metadata extract of the open standards used within various NCOIC patterns.
- Building Blocks Database—A metadata extract of vendor-offered solutions that meet the requirements defined in NCOIC patterns along with specific information on how the product has met NCOIC requirements.

One of the key features of this structure is the ability to capture feedback from the NCOIC user communities. To capture valuable insight into the relevance, effectiveness, and applicability to real-world NCO designs, users' input about each repository is gathered and provided to the teams responsible for the specific pattern, standard, or product.

This organization of repositories and feedback mechanism may provide a useful structure with which to align efforts to facilitate the evolution of the NCA. This review itself could be viewed as an early iteration of such an evolutionary process to improve the NCA.

7 Follow-on Work

As indicated in Sections 2.3.2, 3, and 5, NCOIC intends to pursue an extension of this review and related work to meet the intent of the NCA for the larger community interested in using them. In particular, the following items have been identified as follow-on work for NCOIC:

- A candidate replacement for Social and Cognitive Integration.
- A mapping of the NCOIC Core Net-Centric Principles to the recommended NCA along with explanation of the derivation(s).
- Further development of assessment contexts together with application guidance.
- Mapping from the NCA together with assessment contexts to the various NCOIC products, including SCOPE™ and NCAT™.

NCOIC has completed a draft of its Core Net-Centric Principles listed in Section 4.1.1. In addition, NCOIC intends to provide the basis for, extension of, and direction for use, especially with the replacement candidate attributes, of assessment contexts. Part of the proposed extension of assessment contexts is their relation to the SCOPE™ model, the NCAT™ tool and its profiles, and the overall NCOIC integrated process for using its products.

In undertaking this work, NCOIC understands it will provide a rational and consistent mechanism for communities interested in net-centricity and interoperability to communicate requirements, expectations, and results of and for systems development.

8 Conclusions

The ASD(NII)/DoD CIO NCA are an effort to represent important characteristics of a net-centric system or program in the context of acquisition. The NCA have proven to be of value in the DoD's net-centric transformational efforts.

In giving this task to the NCOIC, DoD and DISA have afforded NCOIC an important opportunity to make a bridge between US DoD perspectives and international perspectives toward net-centricity. It is hoped that this review, together with the follow-on work of NCA and their derivation from NCOIC Core Net-Centric Principles and to SCOPE™ and NCAT™ profiles, will provide the basis for additional structured analysis and subsequent decision processes supporting net-centricity.