Appendix B: DoD IEA Principles and Business Rules (OV-6a)

The set of principles and rules aligned with IE capabilities in Section 9.4 were taken from previous versions of the DoD IEA and from operational outcomes for the IE defined by the GIG 2.0 ORA. This Appendix provides a complete list of these Principles and Rules as defined and numbered in their original source documents. Future versions of the DoD IEA will re-order and possibly re-number these principles and rules.

DoD IEA Global Principles (GP)

- **GP 01** – Department of Defense (DoD) Chief Information Office (CIO)-governed resources are conceived, designed, operated, and managed to address the mission needs of the Department.
- **GP 02** - Interoperability of solutions across the Department is a strategic goal. All parts of the Global Information Grid (GIG) must work together to achieve this goal. Information is made interoperable by following the rules for net-centric sharing of data and services across the enterprise. The DoD achieves infrastructure interoperability through definition and enforcement of standards and interface profiles and implementation guidance.
- **GP 03** - Data assets, services, and applications on the GIG shall be visible, accessible, understandable, and trusted to authorized (including unanticipated) users.
- **GP 04** - DoD CIO services shall advertise service-level agreements (SLAs) that document their performance, and shall be operated to meet that agreement.
- **GP 05** - The GIG will provide a secure environment for collaborative sharing of information assets (information, services, and policies) with DoD's external partners, including other Federal Departments and Communities of Interest (e.g., Department of Homeland Security, the Intelligence Community), state and local governments, allied, coalition, non-governmental organizations (NGOs), academic, research, and business partners.
- **GP 06** - The DoD Information Enterprise (IE) will include global access to common DoD-wide capabilities and services that enable access to people and information resources from any computer in the world. To the extent possible, services shall be developed for global use. The use of these globally accessible services will improve warfighting effectiveness, and interoperability, while reducing cost.

Data & Services Deployment (DSD)

Data & Services Deployment Principles (DSDP)

- **DSDP 01** - Data, services, and applications belong to the enterprise. Information is a strategic asset that cannot be denied to the people who need it to make decisions.
- **DSDP 02** - Data, services, and applications should be loosely coupled to one another. The interfaces for mission services that an organization provides should be independent of the

underlying implementation. Likewise, data has much greater value if it is visible, accessible and understandable outside of the applications that might handle it.

- **DSDP 03** - Only handle information once (the OHIO principle). Information that exists should be reused rather than recreated.
- **DSDP 04** - Semantics and syntax for data sharing should be defined on a community basis. Information sharing problems exist within communities; the solutions must come from within those communities.
- **DSDP 05** - Data, services, and applications must be visible, accessible, understandable, and trusted by "the unanticipated user". All needs can never be fully anticipated. There will inevitably be unanticipated situations, unanticipated processes, and unanticipated partners. By building capabilities designed to support users outside of the expected set, the Department can achieve a measure of agility as a competitive advantage over our adversaries.

Data & Services Deployment Business Rules (DSDR)

- **DSDR 01** - Authoritative data assets, services, and applications shall be accessible to all authorized users in the Department of Defense, including Joint, interagency, inter-governmental, and multinational partners, and accessible except where limited by law, policy, security classification, or operational necessity.
- **DSDR 02** - All authoritative data producers and capability providers shall describe, advertise, and make their data assets and capabilities available as services on the GIG.
- **DSDR 03** - All authoritative data assets and capabilities shall be advertised in a manner that enables them to be searchable from an enterprise discovery solution.
- **DSDR 04** - Data will be described in accordance with the enterprise standard for discovery metadata (the DoD Discovery Metadata Specification [DDMS]).
- **DSDR 05** - Communities of Interest (COIs) will determine which data sources are authoritative and will not declare any source authoritative without establishing a valid pedigree.
- **DSDR 06** - Mission or business functions will be made available to the enterprise as a network-based service with a published, well-defined interface.
- **DSDR 07** - Services shall be advertised by registering with an enterprise service registry.
- **DSDR 08** - COIs should develop semantic vocabularies, taxonomies, and ontologies.
- **DSDR 09** - Semantic vocabularies shall re-use elements of the DoD Intelligence Community-Universal Core or National Information Exchange Model (NIEM) information exchange schema.
- **DSDR 10** - Vocabularies, taxonomies, and ontologies must be registered with the enterprise for visibility, re-use, and understandability.
- **DSDR 11** - Existing enterprise data, services, and end-user interfaces shall be used whenever possible, practical, and appropriate, instead of re-creating those assets.
- **DSDR 12** - Available Mandatory Core Designated DoD Enterprise Services, as listed in

Appendix G, are mandatory for use regardless of capability delivered.

Secured Availability (SA)

Secured Availability Principles (SAP)

- **SAP 01** - The GIG is critical to DoD operations and is a high-value target for many highly motivated and well-equipped adversaries. As such, it must be conscientiously designed, managed, protected, and defended.
- **SAP 02** - The globalization of information technology, particularly the international nature of hardware and software (including supply chain) development and the rise of global providers of Information Technology (IT) and communications services presents a very new and unique security challenge. GIG resources must be designed, managed, protected, and defended to meet this challenge.
- **SAP 03** - Global missions and globally dispersed users require global network reach. Information Assurance mechanisms and processes must be designed, implemented, and operated so as to enable a seamless DoD Information Enterprise.
- **SAP 04** - Agility and precision are the hallmark of 21st century national security operations. Information Assurance mechanisms and processes must be designed, implemented, and operated so as to enable rapid and precise changes in information access and flow, and resource allocation or configuration.

Secured Availability Business Rules (SAR)

- **SAR 01** - DoD information programs, applications, and computer networks shall protect data in transit and at rest according to their confidentiality level, Mission Assurance category, and level of exposure.
- **SAR 02** - GIG infrastructure, applications and services, network resources, enclaves, and boundaries shall be capable of being configured and operated in accordance with applicable policy. Such policy must address differences in enterprise-wide, system high, community of interest, enclave, and operational mission needs.
- **SAR 03** - DoD information services and computer networks shall be monitored in accordance with pertinent GIG-wide SLAs in order to detect, isolate, and react to intrusions, disruption of service, or other incidents that threaten DoD operations.
- **SAR 04** - DoD programs must clearly identify and fund Information Assurance (IA) management and administration roles necessary for secure operation and maintenance of the program. Additionally, provision must be made for adequate training of all users in secure operation.
- **SAR 05** - GIG assets must establish and implement a Mission Assurance capability that addresses hardware, software, and supplier assurance through engineering and vulnerability assessments.
- **SAR 06** - All DoD services that enable the sharing or transfer of information across multiple security levels shall be centrally planned and coordinated, with proposed service enhancements considered first at the enterprise-wide level, then at the regional/organizational

level (e.g., DoD Component), then at the service or application level.

- **SAR 07** - All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices. These services, applications, and networks shall enforce authorized access to information and other services or devices according to specified access control rules and quality of protection requirements for all individuals, organizations, COIs, automated services, and devices.
- **SAR 08** - Metadata containing access control and quality of protection attributes shall be strongly bound to or associated with information assets and utilized for access decisions.
- **SAR 09** - DoD programs must demonstrate that their network, data assets, services, and applications and device settings that control or enable IA functionality have been established, documented, and validated through a standard security engineering process.
- **SAR 10** - DoD programs should ensure that configuration changes to networks, data assets, services, applications, and device settings can be automatically disseminated and implemented in conformance with GIG-standard configuration processes.

Shared Infrastructure (SI)

Shared Infrastructure Principles (SIP)

- **SIP 01** - GIG infrastructure capabilities must be survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster.
- **SIP 02** - The GIG shall enable connectivity to all authorized users.
- **SIP 03** - GIG infrastructure must be scalable, changeable, deployable, and rapidly manageable while anticipating the effects of the unexpected user.

Shared Infrastructure Business Rules (SIR)

- **SIR 01** - GIG infrastructure resources shall be discoverable, and available to both meet the dynamic demand of all mission requirements and support the monitoring and management of the GIG.
- **SIR 02** - GIG infrastructure capabilities shall be designed, acquired, deployed, operated, and managed in a manner which enables continuity of operations and disaster recovery in the presence of attacks, failures, accidents, and natural or man-made disaster to support customer SLAs.

Computing Infrastructure Readiness (CIR)

Computing Infrastructure Readiness Principles (CIRP)

- **CIRP 01** - Computing infrastructure must support all missions of the Department, and provide the edge with effective, on-demand, secure access to shared spaces and information assets across functional, security, national, and interagency domains.
- **CIRP 02** - Consolidation of computing infrastructure fixed-node operations is a desired result for cost efficiencies. It shall not be accomplished, however, at the expense of

degrading mission capabilities and operational effectiveness.

- **CIRP 03 -** Computing infrastructure must be able to provide secure, dynamic, computing platform-agnostic and location-independent data storage.
- **CIRP 04 -** Computing infrastructure hosting environments must evolve and adapt to meet the emerging needs of applications and the demands of rapidly increasing services.

Computing Infrastructure Readiness Business Rules (CIRR)

- **CIRR 01 -** Computing infrastructure shall be consolidated, to the greatest extent possible, so that fixed global/regional and deployed virtual CI resources are used efficiently.
- **CIRR 02** - Computing infrastructure shall be computing platform agnostic and location independent in providing transparent real-time provisioning and allocation of shared resources.
- **CIRR 03 -** Computing infrastructure shall be responsive to and supportive of the capability needs and requirements of the edge environment, despite intermittent connectivity or limited bandwidth.
- **CIRR 04** - Physical implementation of computing infrastructure shall include transparent interfaces to users to minimize, if not eliminate, degradation in performance and Quality of Service.
- **CIRR 05** - Computing infrastructure capabilities must be robust and agile to respond to increased computing demand, data storage, and shared space requirements.
- **CIRR 06** - Shared computing and data storage resources shall be capable of being discoverable and accessible for virtual management and control across the GIG.
- **CIRR 07** - All GIG computing infrastructure facilities must be accredited, certified, and approved by DoD designated authorities.

Communications Readiness (CR)

Communications Readiness Principles (CRP)

- **CRP 01 -** The GIG communications infrastructure shall support full Internet Protocol (IP) convergence of traffic (voice, video, and data) on a single network.

Communications Readiness Business Rules (CRR)

- **CRR 01** - Implement a modular, layered design based on internet protocol for the transport infrastructure.
- **CRR 02** - GIG communications systems shall provide network connectivity to end points (such as Wide and Local Area Networks and direct connections to mobile end-users) in the same or different autonomous systems.
- **CRR 03 -** GIG communications systems shall be acquired to support migration to a Cipher Text (CT) core. CT networks and segments shall transport both classified and unclassified encrypted traffic.

- **CRR 04 -** GIG communications systems shall provide the flexibility to support network connectivity to all GIG nodes and users, including those changing their points of attachment among alternate operational and network domains and/or communities of interest.
- **CRR 05 -** GIG communications systems shall be designed and configured to be robust, adaptive, and reliable by employing network and configuration management, diverse path cable routing, and automatic rerouting features, as applicable.
- **CRR 06 -** Spectrum Management shall incorporate flexible, dynamic, non-interfering spectrum use.

NetOps Agility (NOA)

NetOps Agility Principles (NOAP)

- **NOAP 01 -** DoD shall operate and defend the GIG as a unified, agile, end-to-end information resource.
- **NOAP 02 -** Share NetOps information with the enterprise by making NetOps data, services, and applications visible and accessible and enable NetOps data to be understandable and trusted to authorized users.

NetOps Agility Business Rules (NOAR)

- **NOAR 01 -** The DoD must continue to transform the Network Operations (NetOps) Command and Control (C2) into a unified and agile construct with centralized direction and decentralized execution to effectively respond to unanticipated situations on the time scale of cyber attack.
- **NOAR 02 -** The DoD must ensure NetOps functions of Enterprise Management, Content Management, and Network Defense are fully integrated within and across all management domains.
- **NOAR 03 -** The DoD must conduct GIG NetOps functions at all operational levels (strategic, operational, and tactical).
- **NOAR 04 -** GIG programs must address relevant capabilities for achieving NetOps Agility in Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities.
- **NOAR 05 -** Applicable GIG programs must ensure products and services provide the capability to allow a high degree of automation for NetOps C2, and must support dynamic adjustment of configuration and resource allocation.
- **NOAR 06 -** GIG resources to include computing infrastructure, communications systems, IA, and services must be NetOps-enabled to provide operational states, performance, availability, and security data/information enabling enterprise-wide situational awareness and performance management to GIG-wide SLAs.
- **NOAR 07 -** NetOps metrics shall be developed to measure the health and readiness of DoD data assets, services, and applications in support of the Department’s missions.

GIG 2.0 ORA-Derived Operational Rules (OPR)

Global Authentication, Access Control, and Directory Services Rules

- **OPR 01** – All authorized entities will have one identity and universal credentials that are recognized by all producers of information and services.
- **OPR 02** – All authorized entities will have timely access to critical data, services, and applications from anywhere in the IE.
- **OPR 03** – Enterprise-level directory services will preserve cross domain security while satisfying information transfer requirements.
- **OPR 04** – A comprehensive security policy will be developed that addresses all aspects of Identity Management and Authentication (IdM&A) and provides for realistic opportunities to enforce the greater IA policy requirements.
- **OPR 05** – Design and implement a single authentication mechanism that is usable across the IE regardless of Service affiliation, role, and/or deployment status.
- **OPR 06** – Implement a digital attribute based approach for granting access to information integrated with an overall IA policy and single authentication mechanism approach.

Information and Services "From the Edge" Rules

- **OPR 07** – Tactical edge users are the initial focus for requirements of any operational support activity or program development.
- **OPR 08** – Data is tagged to support rapid smart-push to the edge user based on location, community of interest, and mission.
- **OPR 09** – Edge users have direct information sharing capabilities with peers in and outside their immediate organization, with central processing for their mission, and with strategic assets per their mission requirements.
- **OPR 10** – Provide for the availability of IT capabilities throughout the IE to any authorized user and are easily discoverable through queries and proactive smart-push services.
- **OPR 11** – Develop an information infrastructure based on common standards to support collaboration and information sharing.
- **OPR 12** – Develop end-user services that can be tailored to warfighter needs for specific missions and locations.
- **OPR 13** – Provide roaming profiles optimized to warfighter environment which allows access to their information and services (e.g. data files, personal files, calendar, contact list, email, etc).
- **OPR 14** – All IT services and information stores will be implemented as visible, accessible, understandable, and trusted to authorized (including unanticipated) users.

Joint Infrastructure Rules

- **OPR 15** – Consolidate infrastructure to enable seamless information sharing and increased speed of action.

- **OPR 16 –** Shift away from the service-centric network construct to an operationally focused construct.
- **OPR 17** – Provide a self managed computing infrastructure limiting the need for human intervention and enabling the optimization of computing infrastructure resources.
- **OPR 18** – Provide a single, secure, and consolidated network domain.
- **OPR 19** – Develop an overarching infrastructure acquisition strategy (hardware, software, etc) and enforce common computing infrastructure standards.
- **OPR 20** – Provide standard extensions, or common gateways, for integration between network domains to enable internal and external collaboration.
- **OPR 21** – Establish Combatant Command (CCMD)-aligned network service centers to shift from Service-centric network construct to an operational (i.e., regional) construct.

Common Policies and Standards Rules

- **OPR 22** – Develop effective enterprise guidance that mandates the fielding and management of common, joint infrastructure.
- **OPR 23** – Develop enterprise acquisition and certification to ensure IE components are purchased and acquired so they are interoperable and universally certified.
- **OPR 24** – Develop common standards and policies that serve as enforcement mechanisms to ensure interoperability.
- **OPR 25** – Develop policies and strategies for providing a joint training approach, the acquisition of IE capabilities, and the evolution of the IE.
- **OPR 26** – Develop a common set of functional policies so that all components of each IE program or system are developed, tested, certified, and deployed with an emphasis on end-to-end enterprise commonality.
- **OPR 27** – Analyze DoD Certification and Accreditation (C&A) policy to address current challenges resulting from multiple Designated Approving Authorities (DAA).
- **OPR 28** – Provide and enforce common standards that are utilized across all services to enable any user at the edge to access the data he/she needs from interoperable systems and services.

Unity of Command Rules

- **OPR 29** – Provide system and network availability, information protection, and information delivery providing the right information to the edge.
- **OPR 30** – Provide effective command and control of the IE through situational awareness of a seamless information environment.
- **OPR 31** – Develop a more agile and integrated force by means of a unified training approach.

- **OPR 32** – Develop, distribute, and assess common guidance regarding CyberCom and Joint Force Commander (JFC) intent for the operation of the IE in a given Area of Responsibility (AoR) to achieve overall unity of effort.
- **OPR 33** – Provide CyberCom with full situational awareness of the IE through common processes, standards and instrumentation, enabling near real-time manipulation of any asset in order to optimize net-centric services.
- **OPR 34** – Realign the necessary C2 relationships to provide joint C2 of the network, including the electromagnetic spectrum, within the battlespace, thus, allowing the commander to focus on the principle warfighting task.
- **OPR 35** – Assign the command of the network within a given theater to the JFC to mitigate operational risk.
- **OPR 36** – Allow the commander to adopt common policies and standards through a common training regimen.