

NCOW RM v1.2 ACTIVITY DEFINITIONS

CONTROL AND MANAGE THE GLOBAL INFORMATION GRID (GIG)

Activity Name	Activity Definition
Acquire Situational Awareness Data	<p>The activity of an agent in (1) collecting sensor data, (2) collecting audit data, and (3) collecting SA reports.</p> <p>Amplification: Data regarding the condition of information assurance, network operations, network management, and other GIG operations comprise situational awareness data. Includes data within and external to the GIG that is relevant to SA and CND.</p>
Administer Access Control Policy	<p>The activity of an agent in (1) administering attributes policy, (2) administering identity policy, and (3) administering credential policy, (4) administering authorization policy, and (5) administering authentication policy.</p> <p>Amplification: This activity focuses on the management, application and execution of all policies regarding access control. Activities for Access Control policy development occur in the "Evolve the GIG" model.</p>
Administer Attributes Policy	<p>The activity of an agent in managing, applying and executing policies regarding resource, subject and group attributes.</p> <p>Amplification: Activities for Attributes policy development occur in the "Evolve the GIG" model.</p>
Administer Audit Policy	<p>The activity of an agent in managing, applying and executing policies regarding audit.</p> <p>Amplification: Activities for Audit policy development occur in the "Evolve the GIG" model.</p>
Administer Authentication Policy	<p>The activity of an agent in (1) participating in authentication federation and (2) managing authentication interfaces.</p> <p>Amplification: This activity involves managing, applying and executing policies regarding authentication. Activities for Authentication policy development occur in the "Evolve the GIG" model.</p>
Administer Authorization Policy	<p>The activity of an agent in (1) participating in authorization federations and (2) managing authorization interfaces.</p> <p>Amplification: This activity involves managing, applying and executing policies regarding privileges. Authorization policies also address the resolution of ambiguous policies across security domains, privileges for sharing information across security domains, and express the constraints for having a privilege. Activities for Authorization policy development occur in the "Evolve the GIG" model.</p>
Administer CND Policy	<p>The activity of an agent in managing, applying and executing policies for defending the GIG environment.</p> <p>Amplification: This activity involves setting security parameters in accordance with policy and operational guidance and setting both static and dynamic protection-policy parameters in servers, workstations, and device security management information databases. These parameters ensure protection-policy enforcement for operating systems, database management systems, networks, services, and applications. The activity also includes configuring crypto devices with keys and algorithms. Activities for CND policy development occur in the "Evolve the GIG" model.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Administer Configurations Policy	<p>The activity of an agent in managing, applying and executing policies for configuring systems and networks.</p> <p>Amplification: The activity includes configuring crypto devices with keys and algorithms and covers the rules and restrictions for who is authorized to make configuration changes. Activities for Configurations policy development occur in the "Evolve the GIG" model.</p>
Administer Credential Policy	<p>The activity of an agent in managing, applying and executing policies for issuing and maintaining credentials.</p> <p>Amplification: When participating in a credential federation, a credential manager performs tasks within this activity in order to integrate policy required by the federation. Activities for Credential policy development occur in the "Evolve the GIG" model.</p>
Administer Cross Domain Sharing Policy	<p>The activity of an agent in managing, applying and executing policies for sharing information and resources across domains.</p> <p>Amplification: This includes the resolution of policy ambiguity. Activities for Cross Domain Sharing policy development occur in the "Evolve the GIG" model.</p>
Administer Federation Policy	<p>The activity of an agent in managing, applying and executing policies established for a federation.</p> <p>Amplification: Includes facilitating the negotiations among federation members for consolidation and resolving ambiguities of GIG policies with other federation member policies. Also publishes and maintains configuration control on collaboratively established policies. Activities for Federation policy development occur in the "Evolve the GIG" model.</p>
Administer GIG Policy	<p>The activity of an agent in (1) administering access control policy, (2) administering protection policy, (3) administering sharing policy, (4) administering network management policy, and (5) administering service oriented policy.</p> <p>Amplification: This activity focuses primarily on the management, application and execution of policies. Activities for policy development occur in the "Evolve the GIG" model.</p>
Administer Identity Policy	<p>The activity of an agent in managing, applying and executing policies for registering and maintaining identities of agents.</p> <p>Amplification: When participating in an identity federation, an identity manager performs tasks within this activity in order to integrate policy and interface changes required by the federation. Identifying attributes are defined by an activity associated with the type of entity being identified (e.g. resources, subjects, groups). Activities for Identity policy development occur in the "Evolve the GIG" model.</p>
Administer Key Management Policy	<p>The activity of an agent in managing, applying and executing policies regarding the full life cycle of cryptographic material.</p> <p>Amplification: When participating in a federation, a key manager performs tasks within this activity in order to integrate policy required by the federation. Activities for Key Management policy development occur in the "Evolve the GIG" model.</p>
Administer Network Management Policy	<p>The activity of an agent in managing, applying and executing policies for the management of networks.</p> <p>Amplification: Activities for Network Management policy development occur in the "Evolve the GIG" model.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Administer Protection Policy	<p>The activity of an agent in (1) administering key management policy, (2) administering audit policy, (3) administering CND policy, (4) administering situational awareness policy, and (5) administering configurations policy.</p> <p>Amplification: This activity focuses on the management, application and execution of policies for protecting and defending the GIG. Activities for Protection policy development occur in the "Evolve the GIG" model.</p>
Administer Service Oriented Policy	<p>The activity of an agent in managing, applying and executing policies regarding a service oriented environment.</p> <p>Amplification: This activity includes policy for the SOA foundation, development of services, and implementation of services throughout the GIG. Activities for Service Oriented policy development occur in the "Evolve the GIG" model.</p>
Administer Sharing Policy	<p>The activity of an agent in (1) administering cross-domain sharing policy and (2) administering federation policy.</p> <p>Amplification: This includes policies for sharing information and resources. This activity focuses on the management, application and execution of sharing policies. Activities for Sharing policy development occur in the "Evolve the GIG" model.</p>
Administer Situational Awareness Policy	<p>The activity of an agent in managing, applying and executing policies for acquiring, processing and posting Situational Awareness data.</p> <p>Amplification: It involves setting security parameters in accordance with policy and operational guidance and setting both static and dynamic protection-policy parameters in servers, workstations, and device security management information databases. These parameters ensure protection-policy enforcement for operating systems, database management systems, networks, services, and applications. Activities for Situational Awareness policy development occur in the "Evolve the GIG" model.</p>
Advertise Catalog	The activity of an agent in making an information product catalog known.
Allocate Channels	The activity of an agent in allocating satellite communications channels to users.
Analyze Incident Data	The activity of an agent in studying incident data to determine the validity, significance, and level of impact of the incident.
Analyze Response Options	<p>The activity of an agent in developing and studying the potential responses to determine the advantages and disadvantages of each.</p> <p>Amplification: The results of this analysis are used to determine the best response for the situation.</p>
Analyze Response Results	The activity of an agent in studying the results of a response to determine the validity, significance and level of impact the response had on the given situation.
Analyze Threat Data	The activity of an agent in studying threat data to determine the validity, significance and level of impact of the threat.
Analyze Vulnerability Data	The activity of an agent in studying vulnerability data to determine the validity, significance and level of impact of the vulnerability.
Archive Audit Trail	The activity of an agent in placing audit trails into permanent archival storage.
Assess Executed Response	<p>The activity of an agent in (1) collecting response results, (2) analyzing response results, and (3) developing a response assessment.</p> <p>Amplification: The assessment is used to determine if further responses are required.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Assess GIG Situation	<p>The activity of an agent in (1) assessing threats to the GIG, (2) assessing vulnerabilities of the GIG, (3) assessing incidents in the GIG, and (4) assessing the executed response.</p> <p>Amplification: This activity results in threat, vulnerability, and incident assessments that are used to determine the appropriate response. Many of the threats, vulnerabilities, and incidents are identified during the monitoring of the GIG.</p>
Assess Incidents in the GIG	<p>The activity of an agent in (1) collecting incident data, (2) analyzing incident data, and (3) developing an incident assessment.</p> <p>Amplification: Incidents may be expected or unexpected. Many of these incidents are identified during the monitoring of the GIG situation.</p>
Assess Threats to the GIG	<p>The activity of an agent in (1) collecting threat data, (2) analyzing threat data, and (3) developing a threat assessment.</p> <p>Amplification: The result of this activity is a threat assessment that clearly identifies and describes the threats originating inside and outside of the GIG, and their potential risks. This assessment is necessary to determine the best course of action in response to the threat. Various types of agents, from human to automation, may be used to perform this activity. Many of these threats are identified during the monitoring of the GIG.</p>
Assess Vulnerabilities of the GIG	<p>The activity of an agent in (1) collecting vulnerability data, (2) analyzing vulnerability data, and (3) developing a vulnerability assessment.</p> <p>Amplification: Vulnerabilities may exist in hardware and software and include viruses, trojan horses, malicious codes, unauthorized access, and illegal back doors to name a few. Red Teams and testing may be used to provide data supporting these assessments. Many of these vulnerabilities are identified during the monitoring of the GIG.</p>
Assign a Frequency Lease	The activity of an agent in assigning a Frequency Lease.
Assign a Frequency License	<p>The activity of an agent in assigning a Frequency License.</p> <p>Amplification: All equipment, following allocation, must obtain a permanent specific operating frequency assignment, a "license to operate", before a user may legally operate or test any spectrum dependent equipment. Assignment requests are evaluated and validated against established criteria and issues resolved submitted for national approval and track progress returned when approved with any changes noted. Temporary assignments are processed similarly. Spectrum planning and management involves the efficient employment of the electromagnetic spectrum to include assignment.</p>
Assign Bandwidth	The activity of an agent in assigning bandwidth.
Assign IA Attributes for Groups	<p>The activity of an agent in determining and assigning attributes and values for attributes to groups.</p> <p>Amplification: Assignment of attributes is based upon policy rules governing the selection, association and setting of those attributes.</p>
Assign IA Attributes to Resource	<p>The activity of an agent in determining and assigning attributes and values for attributes to resources.</p> <p>Amplification: Assignment of attributes is based upon policy rules governing the selection, association and setting of those attributes.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Assign IA Attributes to Subjects	<p>The activity of an agent in determining and assigning attributes and values for attributes to subjects.</p> <p>Amplification: Assignment of attributes is based upon policy rules governing the selection, association and setting of those attributes.</p>
Audit Federation Members for Compliance	<p>The activity of an agent in auditing federation members to ensure compliance with federation policies and interfaces.</p>
Categorize SA Data	<p>The activity of an agent in analyzing SA data to determine the nature of the data and its impact to the operational readiness of the GIG.</p> <p>Amplification: This may include assigning the data to categories indicating level of impact.</p>
Check Subscriber Profile	<p>The activity of an agent in monitoring the subscriber profile for potential issues and deficiencies.</p> <p>Amplification: The Users Profiles can be easily established and dynamically adjusted to allow for better flow of information to the User.</p>
Collect Audit Data	<p>The activity of an agent in (1) conducting audit operations and (2) Receiving/Retrieving SA data from audit operations.</p>
Collect Audit Records	<p>The activity of an agent in collecting all or a selected set of event data to construct security-relevant audit records.</p> <p>Amplification: Subsets of event data are derived from audit instrumentation that is parameterized to enforce the audit portion of a security policy. That is a subset of objects, subjects, or processes may be monitored and event data may be collected on these for auditing purposes.</p>
Collect Incident Data	<p>The activity of an agent in collecting and compiling procedural and technical data about incidents in the GIG.</p>
Collect Response Results	<p>The activity of an agent in collecting and compiling the impact and results of the executed response.</p>
Collect Sensor Data	<p>The activity of an agent in (1) conducting sensor operations and (2) retrieving SA data from sensors to acquire state data reporting on the health and protection of the GIG.</p>
Collect Situational Awareness Reports	<p>The activity of an agent in collecting SA reports from internal and external sources.</p>
Collect Threat Data	<p>The activity of an agent in collecting and compiling data about threats to the GIG, regardless of origin.</p>
Collect Vulnerability Data	<p>The activity of an agent in collecting and compiling procedural and technical data about vulnerabilities of the GIG.</p>
Conduct Audit Operations	<p>The activity of an agent in (1) collecting, (2) creating, (3) examining, (4) archiving, and (5) providing audit information.</p>
Conduct Sensor Operations	<p>The activity of an agent in placing sensors, setting sensor parameters, and observing sensors for indications of attacks, policy violations, anomalies, discrepancies, disruptions, degradations, or failures.</p>
Control and Manage the Global Information Grid (GIG)	<p>The activity of an agent in (1) controlling the Global Information Grid and (2) managing the Net-Centric Environment.</p> <p>Amplification: Command and control actions include the coordination, execution, evaluation, and support of fundamental GIG operations such as monitoring the GIG, maintaining GIG Situational Awareness, defending the GIG, and changing the GIG. Manage actions include the administration and management of policies, resources, and GIG functions and operations. Manage actions also involve the management of systems and networks configurations, maintaining infrastructure, and managing the resources of the GIG.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Control Geographic Dissemination	<p>The activity of an agent in controlling the dissemination of information to a specific geographic area.</p> <p>Amplification: This activity is about content staging; the dissemination management of critical information to the warfighter when and where it is needed. The objective of Content Staging is to make the best use of available distribution resources while still meeting the warfighter's timeliness requirements.</p>
Control the Global Information Grid (GIG)	<p>The activity of an agent in (1) maintaining GIG Situational Awareness, (2) assessing GIG situation, (3) planning response to situation, and (4) responding to situation.</p> <p>Amplification: Operating the GIG involves the command and control of day-to-day operations to monitor, defend, and protect the GIG, and ensure optimal GIG performance. Includes operations for information assurance, network operations, network management, and other GIG functions.</p>
Coordinate Frequency Allocations	<p>The activity of an agent in coordinating and managing the allocation of frequencies.</p> <p>Amplification: Spectrum use of all equipment must be approved before any acquisition, procurement, or contractual action can occur. Spectrum planning and management involves the efficient employment of the electromagnetic spectrum to include allocation. Activities associated with implementing a frequency allocation program are in the "Evolve the GIG" model.</p>
Coordinate Selected Response	<p>The activity of an agent in organizing the actions, resources and conditions necessary to execute the selected response.</p> <p>Amplification: Coordinating the selected response ensures all participants understand the response and all resources and conditions are set to execute response upon direction. Includes coordination of law enforcement and counter intelligence actions as necessary, and mitigates operational impacts.</p>
Correlate SA Data	<p>The activity of an agent in grouping and relating SA data by logical criteria, such as source, type, and destination.</p>
Create Audit Trail	<p>The activity of an agent in organizing the collected audit records into a time-oriented sequence (audit trail) and making them available to other agents for further examination.</p>
Define Group IA Attributes	<p>The activity of an agent in specifying the description, format and acceptable content values for group attributes.</p>
Define Resource IA Attributes	<p>The activity of an agent in specifying the description, format and acceptable content values for resource attributes.</p>
Define Subject IA Attributes	<p>The activity of an agent in specifying the description, format and acceptable content values for subject attributes.</p>
Define Trust Relationship	<p>The activity of an agent in identifying a trust relationship, associated participants, trust models, authorities, contexts for the relationship, and establishing the span of control and the policy for basis of trust.</p> <p>Amplification: A trust model is the basis for an agreement which establishes trust between participants. In establishing context for trust relationships, the context refers to the environment (e.g. NIPRNET, SIPRNET, federated) and purpose for the trust relationship (e.g. sharing information). The authorities to be identified include, for example, identity authorities, credential authorities, attribute authorities, etc. The span of control of an authority defines the community for which the authority is responsible. The policy to be established is the set of rules levied upon participants in the trust relationship.</p>
Deliver Information	<p>The activity of an agent in delivering information to a subscriber.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Detect Relevant SA Events	<p>The activity of an agent in detecting and identifying events related to the operational readiness of the GIG.</p> <p>Amplification: An event is an occurrence, not yet assessed, that may affect the performance of an information system. A relevant SA event is an event that has a potential impact on the posture of the GIG. Primarily the IA and NetOps posture of the GIG.</p>
Develop Incident Assessment	<p>The activity of an agent in developing an assessment of the incident based on the analysis of the collected incident data. Amplification: The incident assessment is one of many assessments used to determine overall risk.</p>
Develop Response Assessment	<p>The activity of an agent in developing an assessment of the executed response based on the analysis of the response results.</p> <p>Amplification: The assessment indicates whether or not the desired results are achieved. If the desired results are not achieved, the process of assessing the GIG situation, determining and planning response and responding may be repeated, if necessary.</p>
Develop Threat Assessment	<p>The activity of an agent in developing an assessment of the threats based on the analysis of the collected threat data.</p> <p>Amplification: The threat assessment is one of many assessments used to determine overall risk.</p>
Develop Vulnerability Assessment	<p>The activity of an agent in developing an assessment of the vulnerability based on the analysis of the collected vulnerability data.</p> <p>Amplification: The vulnerability assessment is one of many assessments used to determine overall risk.</p>
Direct Response	<p>The activity of decision-makers in directing the execution of the selected response.</p> <p>Amplification: A decision-maker may direct response actions such as changes to operational policy, monitoring or protection configurations, and GIG operations and management via written or verbal orders. Information Operations Condition (INFOCON), patch management actions and Time Compliance Network Orders (TCNO) are examples of such directions.</p>
Distribute Key	<p>The activity of an agent in distributing cryptographic material using methods appropriate for the consuming entity.</p>
Establish Community of Interest	<p>The activity of a user in establishing a community of interest around a specific mission.</p> <p>Amplification: COIs may be established in a variety of ways and composed of members from one or more functions and/or organizations as needed to support mission needs. COI formations may occur in a "bottom-up" fashion, through the voluntary cooperation of the participants or "top-down", through an organization's hierarchy. The minimum recommended activity for establishing a COI is to develop a charter and governance structure. Once established, COIs should register in an enterprise federated COI Directory to enable GIG users to discover groups with similar missions.</p>
Examine Audit Trail	<p>The activity of an agent in reviewing, summarizing, grouping, or otherwise analyzing audit trails to provide audit reports.</p>
Execute Directed Response	<p>The activity of an agent in carrying out the response as directed by decision-makers. Execution of the response may include reconfiguration of systems and networks, redirection of resources, modification of processes, and changing policy.</p> <p>Amplification: In carrying out the directed response, agents will perform the appropriate set of actions identified under the 'Manage GIG Operations' activity.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Filter SA Data	<p>The activity of an agent in filtering SA data to remove undesirable data based on user preferences.</p> <p>Amplification: This activity may be performed recursively on SA data before or after any of the other SA data processing activities.</p>
Fuse SA Data	<p>The activity of an agent in combining SA data from one or more sources to achieve a refined characterization of the data.</p> <p>Amplification: This activity involves all SA data that is available.</p>
Generate Key	<p>The activity of an agent in generating cryptographic material in accordance with approved orders.</p> <p>Amplification: Generated material will be labeled and packaged in accordance with policy to support secure distribution and subsequent processing.</p>
Identify Community of Interest	<p>The activity of a user in identifying a community of interest with a similar mission through an automated or manual search.</p> <p>Amplification: Users utilize the capability interface to discover Communities of Interest through the activity "Discover Information Asset." Once located, users should leverage existing communities that support their mission prior to establishing a new COI. If a COI exists that supports a Users mission, they should utilize the activity "Participate in COI" otherwise there may be the need to establish a new one (see "Establish COI").</p>
Identify Response Options	<p>The activity of an agent in identifying potential responses to counteract threats to, vulnerabilities of, incidents in, and day-to-day needs of the GIG.</p> <p>Amplification: This activity takes into account both static and dynamic protection configurations. Identification of possible responses should be based on proactive and reactive evaluation of threat assessments, vulnerability assessments, incident assessments, and other relevant data. Response to identified incidents may be short term; immediate response plans to deal with unexpected events (ad hoc), or may be procedures included in SOP's for specific types of incidents. This activity should also consider potential law enforcement and counter intelligence actions.</p>
Issue Credential	<p>The activity of an agent in issuing credentials to an entity.</p> <p>Amplification: Issuing credentials includes the validation of credential requests, generation of the credential using validated attributes and secure delivery of the credential to the proper entity.</p>
Maintain Credential	<p>The activity of an agent in performing credential maintenance for an issued credential.</p> <p>Amplification: This includes maintenance of credential status (e.g., revocation and expiration) and re-issuance of credentials when authorized by policy (e.g., recovery of lost or locked passwords or recovery of a key encryption certificate).</p>
Maintain GIG Situational Awareness	<p>The activity of an agent in (1) acquiring SA Data, (2) processing SA data, and (3) providing SA data.</p> <p>Amplification: Data regarding the condition of information assurance, network operations, network management, and other GIG operations comprise situational awareness data. This activity acquires information feeds from across and external to the GIG to assess the health and readiness of the GIG to support ongoing and planned future operations. Involves the monitoring of GIG network resources, including satellites, fiber, and wireless segments.</p>
Maintain Identity	<p>The activity of an agent in maintaining the identifying attributes and other identity data within the identity manager's scope of responsibility.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Maintain Key	<p>The activity of an agent in maintaining cryptographic material.</p> <p>Amplification: This includes key backup and recovery, key update or replacement, key destruction and key compromise notification and recovery.</p>
Maintain Optimal GIG Performance	<p>The activity of an agent in maintaining a desirable level of GIG performance at all times.</p> <p>Amplification: GIG performance includes the performance associated with all GIG operations and associated resources.</p>
Make Credential Information Available	<p>The activity of an agent in making credential information (e.g., status, strength) visible and accessible.</p>
Make Group IA Attributes Available	<p>The activity of an agent in making group IA metadata information visible and accessible.</p>
Make Identity Information Available	<p>The activity of an agent in making identity information visible and accessible.</p>
Make Resource IA Metadata Available	<p>The activity of an agent in making resource IA metadata information visible and accessible.</p>
Make Subject IA Metadata Available	<p>The activity of an agent in making subject IA metadata information visible and accessible.</p>
Manage Authentication Interface	<p>The activity of an agent in managing the definition and creation of authentication interfaces.</p>
Manage Authority Representation	<p>The activity of an agent in managing the types and formats for supported trust Mechanisms and trust Infrastructures.</p> <p>Amplification: Includes establishing the mechanisms used to represent the authorities (e.g., PKI trust anchor), making requests to appropriate agencies to create/bind mechanisms to authorities, and making representations of authority available.</p>
Manage Authorization Interface	<p>The activity of an agent in managing the definition and creation of authorization policies and interfaces.</p> <p>Amplification: This includes resolution of ambiguities in policies across security domains, establishing policies for sharing information across security domains, and authorization policy expresses the constraints for having a privilege.</p>
Manage Community of Interest	<p>The activity of a user in managing a community of interest by identifying a governing body, communicating with stakeholders, and providing leadership and direction to the COI.</p> <p>Amplification: COI management and governance activities are integral to ensuring that COIs achieve their mission. Although these activities will be tailored to the individual COI's mission and the membership, there are basic issues that a COI should address. These issues include, but are not limited to, information flow, issue adjudication, prioritization of COI activities, quality assurance, recommendations to portfolio managers, and configuration management (CM) of COI products. COI management is responsible for establishing governance processes and structures appropriate to the COI. This effort includes leveraging existing processes and structures where possible and appropriate. This definition was developed using DoD 8320.02-G.</p>
Manage Credentials	<p>The activity of an agent in (1) participating in credential federations, (2) issuing credentials, (3) maintaining credentials, and (4) making credential information available.</p> <p>Amplification: Participation in credential federations should occur at the level necessary to support information sharing goals. This includes the management of identity authentication credentials, attribute credentials, and attribute authentication credentials.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Manage Cryptographic Device and Process Accounting	The activity of an agent in managing the association of cryptographic devices and processes with individuals responsible for their protection and tracking of their location.
Manage Cryptographic Device and Process Configuration	The activity of an agent in (1) managing cryptographic device and process accounting, (2) managing cryptographic device and process initialization, and (4) managing dynamic algorithm changes for cryptographic devices and processes.
Manage Cryptographic Device and Process Initialization	The activity of an agent in creating and distributing trust anchors and instructions required for the initialization and re-initialization of cryptographic devices and processes.
Manage Discovery Metadata	<p>The activity of a user in managing discovery metadata to ensure alignment with its underlying information assets.</p> <p>Amplification: Changes to DDMS structure is scheduled and released to support alignment with DoD-wide discovery of information assets. Automated processes should be utilized whenever possible to maintain discovery metadata.</p>
Manage Dynamic Algorithm Changes for Cryptographic Devices and Processes	The activity of an agent in creating and providing instructions for aligning cryptographic algorithms with mission needs.
Manage Federation Information Exchange Requirements	<p>The activity of an agent in facilitating negotiations between federation members on information exchange requirements and representation.</p> <p>Amplification: This activity publishes and maintains configuration control of established interface exchange requirements.</p>
Manage Federation Membership	The activity of an agent in identifying, controlling and managing the members of a federation.
Manage Federations	The activity of an agent in (1) managing federation membership, (2) managing federation information exchange requirements, and (3) auditing federation members for compliance.
Manage Frequencies	<p>The activity of an agent in (1) coordinating frequency allocations, (2) assigning a frequency license, (3) assigning a frequency lease, (4) processing bandwidth allocation and response requests.</p> <p>Amplification: Management of the electromagnetic frequency spectrum includes RF, ultraviolet, infrared, etc. Includes ad-hoc wireless networks, and management of broadcast schedules and allocation of communications channels. This activity identifies the number of frequencies needed for each radio type that will be required to conduct a military mission. A list of radio types includes, but is not limited to: communications, satellite ground terminals, RF tags, munitions, radars, sensors, Identify Friend or Foe (IFF) transponders, telemetry, geo-location & navigation, autonomous unmanned vehicles (Air & Ground) controls, and sensor systems.</p>
Manage GIG Resources	The activity of an agent in (1) managing IA resources, (2) managing trust relationships, (3) managing federations, (4) managing systems and networks, (5) managing a service oriented enterprise, (6) managing net-centric information sharing, and (7) recovering GIG resources.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Manage GIG Sensor Grid	<p>The activity of an agent in coordinating and maintaining the systems and networks that enables the monitoring of computing and communications operations within the GIG.</p> <p>Amplification: Involves setting static & dynamic monitoring-policy parameters in servers, workstations, and device monitoring management information databases and sensors. These parameters pertain to monitoring policy adherence in operating systems, database management systems, networks, services, and applications. It includes establishing anomaly, fault, and intrusion detection capabilities, setting anti-virus signatures, setting performance thresholds, data filters, selective auditing (resource, function, and user), and sensor-analyzer inter-communications parameters; and establishing event fusion-correlation capabilities, alarms/alerts handlers, and situation awareness displays. It also includes dynamic adjustments to the monitoring configurations to meet changes in the operational environment and its emergent threats.</p>
Manage GIG Services	<p>The activity of an agent in (1) managing the service interface, (2) managing the service delivery, and (3) managing service execution.</p> <p>Amplification: C/S/As will be the primary developers of GIG services and be responsible for the management of GIG services. The DoD-wide services environment will facilitate the management of GIG services.</p>
Manage Group IA Attributes	<p>The activity of an agent in (1) participating in group attribute federations, (2) defining group IA attributes, (3) assigning IA attributes to groups, and (4) making group IA metadata available.</p> <p>Amplification: This activity involves defining and managing IA attributes associated with groups to include identities, roles, membership requirements and other attributes.</p>
Manage IA Attributes	<p>The activity of an agent in (1) managing resource IA attributes, (2) managing subject IA attributes, (3) managing group IA attributes, and (4) managing identities.</p> <p>Amplification: This activity provides for the definition, dissemination and maintenance of IA attributes related to identities, resources, subjects, and groups.</p>
Manage IA Resources	<p>The activity of an agent in (1) managing IA attributes, (2) managing credentials, and (3) managing cryptographic keys.</p> <p>Amplification: IA resources include all things necessary to support information assurance.</p>
Manage Identities	<p>The activity of an agent in (1) participating in identity federations, (2) registering identities, (3) maintaining identities, and (4) making identity information available.</p> <p>Amplification: Managing identities involves organizing, collecting and managing attributes for the purpose of establishing and maintaining identities. This activity includes the definition, dissemination and maintenance of the attributes related to resources, groups and subjects.</p>
Manage IDM Access Controls	<p>The activity of an agent in enabling the identification and implementation of access controls for information dissemination.</p> <p>Amplification: IDM will enable commanders to inject a dissemination policy that constrains browsing by subordinate commands based on variables such as file size, type, source, resource, classification, or location.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Manage Information Access	<p>The activity of an agent in 1) managing product descriptions, 2) managing subscriber IDM profiles, and 3) managing IDM access controls.</p> <p>Amplification: Information access allows authorized users to access information without knowing its exact location; its format(s); a specific query language to access the information; or the details of ownership, access controls, and protocols. This service also enables commanders to grant access to subordinate elements for specific information elements as well as establish priorities for the use of their allocated information distribution infrastructure.</p>
Manage Information Delivery	<p>The activity of an agent in (1) checking subscriber profile, (2) prioritizing information delivery, (3) optimizing resource use, (4) controlling geographic dissemination, (5) delivering information, and (6) providing delivery notification.</p> <p>Amplification: Information Delivery optimizes the use of GIG information distribution infrastructure resources (communications and storage), applies the commander's priorities and requirements to the use of these resources, manages format translations between source and user systems (if required), and enables a range of services depending on the user profile, the current situation, and the commander's policies.</p>
Manage Information Dissemination and Content Staging	<p>The activity of an agent in (1) providing information awareness, (2) managing information access, and (3) managing information delivery.</p>
Manage Information Flow	<p>The activity of an agent in monitoring, tracking and optimizing information flows.</p> <p>Amplification: IDM will provide mechanisms to identify trends and forecast volume, content, and quality of service based on information and mission requirements. IDM will also provide mechanisms to predict the results of information control policies to optimize available resources consistent with mission priorities.</p>
Manage Information Sharing Infrastructure	<p>The activity of a user in managing the information sharing infrastructure to ensure that it's physical, software and structure are maintained.</p> <p>Amplification: This includes any functional revisions to infrastructure software/hardware, maintenance of the Enterprise discovery interface, and management of changes to the DDMS. Information sharing services should be configuration managed and maintained to support the identified level of service.</p>
Manage Institutionalization of GIG Services	<p>The activity of an agent in managing the processes necessary to exploit GIG services as assets that can be used by the enterprise.</p>
Manage Interoperability Components	<p>The activity of a user in managing the interoperability components using COI-established processes and procedures.</p> <p>Amplification: Information sharing capability owners (i.e. information asset owners, service providers) establish processes and procedures through their COI to manage interoperability components (e.g., key interfaces, information models). Anticipated levels of quality, compatibility, and version management are observed, and the ongoing extensions and/or modifications to defined interoperability elements and models are managed to support minimal impact to current users. Structural metadata used for interoperability is managed through COIs and maintained in a enterprise federated metadata registry (e.g., DoD Metadata Registry).</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Manage Keys	<p>The activity of an agent in (1) participating in key management federations, (2) providing for key ordering, (3) generating keys, (4) distributing keys, (5) tracking and accounting for keys, and (6) maintaining keys.</p> <p>Amplification: Involves all cryptographic devices and processes that support GIG transactions throughout the lifecycle of the material. Key management extends to allied and coalition partners either directly or by means of one or more federations. Participation in federation(s) is expected to the extent necessary to support information sharing goals. Keys can be managed at the individual subject level, at the group level or for one or more members of a group.</p>
Manage Net-Centric Information Sharing	<p>The activity of an agent in (1) providing communities of interest (COI), (2) managing net-centric information sharing resources, and (3) managing information dissemination and content staging.</p>
Manage Net-Centric Information Sharing Resources	<p>The activity of an agent in (1) managing the information sharing infrastructure, (2) managing ontologies, (3) managing interoperability components, and (4) managing discovery metadata.</p> <p>Amplification: Net-Centric information sharing resources are managed to ensure the infrastructure, ontologies, interoperability components and discovery metadata are maintained. This activity supports information dissemination management and content staging. Management processes should include consideration of user feedback so improvements can be integrated into future iterations of information sharing resources. An information sharing capability is composed of information sharing resources.</p>
Manage Ontologies	<p>The activity of a user in managing the ontologies to ensure alignment with changes in the Enterprise-wide ontologies.</p> <p>Amplification: Ontologies are maintained and registered semantic metadata managed to reflect underlying ontologies. Data working groups could be established to manage ontologies (data categorization schemes, thesauruses, vocabularies, key word lists, and taxonomies); with a change control board to manage the revisions as needed. Ontologies should be aligned to support changes in Enterprise-wide ontologies. Metadata registries, directories, and catalogs are updated to reflect updates in associated ontologies.</p>
Manage Product Descriptions	<p>The activity of an agent in identifying and controlling product descriptions.</p> <p>Amplification: Information producers are required to label their products using standardized metadata to include classification. IDM will manage the information and information flows based on the tags established by information producers.</p>
Manage Resource IA Attribute	<p>The activity of an agent in (1) participating in resource attribute federation, (2) defining resource IA attributes, (3) assigning IA attributes to resources, and (4) making resource IA metadata available.</p> <p>Amplification: This activity involves defining and managing IA attributes associated with resources to include pedigree, QoP, classification and metadata representations.</p>
Manage Satellite Communications Subsystem	<p>The activity of an agent in (1) allocating channels, (2) assigning bandwidth, (3) providing access, and (4) managing satellite IP addresses.</p> <p>Amplification: This activity is about managing the day-to-day operations of all apportioned and non-apportioned SATCOM resources. It includes providing appropriate support when disruption of service occurs; providing global SATCOM system status; maintaining global SA to include each Combatant Command's (COCOM's) current and planned operations as well as Space, Control, and Terminal Segment asset and operational configuration management; providing radio frequency interference resolution management; and providing satellite anomaly resolution and management.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Manage Satellite IP Addresses	The activity of an agent in managing IP addresses for satellite communications systems.
Manage Service Delivery	The activity of an agent in ensuring the services mode of delivery adheres to established standards and specifications.
Manage Service Execution	The activity of an agent in maintaining the functionality of a service and ensuring its execution adheres to established standards and specifications.
Manage Service Oriented Enterprise	<p>The activity of an agent in (1) managing the DoD-wide services environment, and (2) managing GIG services.</p> <p>Amplification: The strategy for achieving a service oriented enterprise focuses on two areas: promoting C/S/A GIG service initiatives and establishing a DoD-wide services environment. This activity is about managing the GIG services developed by C/S/A and the DoD-wide services environment established by the DoD Enterprise.</p>
Manage Subject IA Attributes	<p>The activity of an agent in (1) participating in subject attribute federation, (2) defining subject IA attributes, (3) assigning IA attributes to subjects, and (4) making subject IA metadata available.</p> <p>Amplification: This activity involves defining and managing IA attributes associated with subjects to include roles, clearances and other attributes.</p>
Manage Subscriber IDM Profile	<p>The activity of an agent in supporting the establishment of and maintaining a users profile associated with information dissemination.</p> <p>Amplification: IDM will support building profiles that are based on information requests, the commander's IM policy, and information producer's application of appropriate rule sets (e.g. security). IDM will enable profile transferability and reusability, along with automatic recognition of a change in Commander's Dissemination Policy (CDP). IDM will enable a profile management capability to associate past profiles against the associated mission and/or operational environment to provide baseline profiles for future, similar missions, and/or operational environments.</p>
Manage System & Network Configurations	<p>The activity of an agent in (1) managing cryptographic device and process configuration, (2) managing system and network component configurations.</p> <p>Amplification: This activity involves the planning, coordination and controlling of configurations and settings for cryptographic devices, systems and networks associated with information assurance, network operations and network management.</p>
Manage System and Network Component Configurations	<p>The activity of an agent in planning, coordinating and controlling the configurations and settings for system and network components associated with information assurance, network operations and network management.</p> <p>Amplification: Involves the installation, standard security configuration and maintenance of CND sensors and analytical tools, CDS, routers, identity management systems, access control systems, and other non-cryptographic components.</p>
Manage System and Network Faults	<p>The activity of an agent in recovering system and network capabilities from the degrading effects of a failure or attack incident.</p> <p>Amplification: The GIG NM System shall detect faults from a satellite, fiber, or wireless link between satellites, gateway terminal, or connection to gateway terminal. Recovery activities are coordinated to insure minimal interference between recovery and response activities, and may include restoration of capabilities and reconstitution of the affected portion of the information environment. Recovery is dependent upon the overall capabilities for fault tolerance and survivability, and the state of effects resulting from a failure or attack incident.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Manage System and Network Performance	<p>The activity of an agent in monitoring the operational status and use of systems, networks, and storage resources, and maintaining optimal performance for each.</p> <p>Amplification: The GIG NM system shall enable SLAs for network service between the GIG elements and authorized external networks, by providing means to monitor performance against SLAs and to implement QoS and network policies in support of SLAs. Performance information is acquired by collecting, testing, and analyzing configuration information and by assessing operational use to detect disruption and degradation that indicate failures or security problems.</p>
Manage Systems and Networks	<p>The activity of an agent in (1) managing faults, (2) managing performance, and (3) managing configurations of systems and networks.</p> <p>Amplification: The NetOps portion of network management begins when communications are activated. It is a set of activities that keeps the communications switching, transmission and computing resources available to fulfill users' telecommunications demands. It establishes the resources, keeps them operational, tunes their performance, accounts for their usage, and protects the services they provide. It includes the management of strategic and tactical networks, including telephones, IP data networks, SATCOM networks and wireless.</p>
Manage the DoD-Wide Services Environment	<p>The activity of an agent in (1) managing the federation of GIG services, and (2) managing the institutionalization of GIG services.</p>
Manage the Federation of GIG Services	<p>The activity of an agent in managing the necessary standards, specifications, processes, and infrastructure that enable DoD-wide federation of SOAs.</p>
Manage the Global Information Grid (GIG)	<p>The activity of an agent in (1) Administering GIG Policy and (2) Managing GIG Resources.</p> <p>Amplification: This activity involves administering all aspects of GIG policy and all aspects of configuring, maintaining, and dissolving the infrastructure, capabilities, and services of the net-centric environment. It includes the maintenance of infrastructure, services, and capabilities, the management of system and network configurations, and the administration of all resources and policies.</p>
Manage the Service Interface	<p>The activity of an agent in ensuring the service interface adheres to established standards and specifications.</p>
Manage Trust Relationship	<p>The activity of an agent in (1) defining a trust relationship and (2) managing authority representations.</p>
Optimize Resource Use	<p>The activity of an agent in optimizing the use of resources to ensure resources of the information environment are properly allocated in a manner that preserves control of the environment's performance in meeting its various user-needs.</p> <p>Amplification: The allocation function operates to control the utilization of resources available within the information environment. It balances the need to maximize support to all users with the requirement to provide full support to mission-critical operations. It takes as its input a set of invocation parameters (e.g., resource requests) and, based upon the policy rule set and parameters available from the target resource manager, provides an authorization decision that includes allocating the requested resources to meet the policy-constrained needs of the invocation. Also involves the setting of parameters and thresholds.</p>
Participate in Authentication Federation	<p>The activity of an agent in obtaining, maintaining and terminating membership in one or more authentication federations.</p> <p>Amplification: Includes participation of federation members to negotiate interface requirements for authentication.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Participate in Authorization Federation	<p>The activity of an agent in obtaining, maintaining and terminating membership in one or more authorization federations.</p> <p>Amplification: Includes participation of federation members to negotiate policies and interface requirements for authorization.</p>
Participate in Community of Interest	<p>The activity of a user in participating in a community of interest.</p> <p>Amplification: Users participate in COIs that have a shared mission and identify COIs for participation through the "Identify COI" activity. DoDD 8320.2 encourages active participation in Communities of Interest to support achieving the goals of the Net-Centric Data Strategy. Semantic and structural agreements for information sharing are achieved through the active commitment of COI member's time, resources and expertise to accomplishing the mission of the COI.</p>
Participate in Credential Federation	<p>The activity of an agent in obtaining, maintaining and terminating membership in one or more credential federations.</p> <p>Amplification: This activity also includes participation of federation members to negotiate policies and interface requirements for credential management.</p>
Participate in Group Attribute Federation	<p>The activity of an agent in obtaining, maintaining, and terminating membership in one or more group federations.</p> <p>Amplification: This activity also includes participation of federation members to negotiate policies and interface requirements for group attribute management.</p>
Participate in Identity Federation	<p>The activity of an agent in obtaining, maintaining and terminating membership in one or more identity federations.</p> <p>Amplification: This activity also includes participation of federation members to negotiate policies and interface requirements for identity management.</p>
Participate in Key Management Federation	<p>The activity of an agent in obtaining, maintaining and terminating membership in key management federations.</p> <p>Amplification: This activity includes negotiation of policies and interface requirements for key management required between federation members.</p>
Participate in Resource Attribute Federation	<p>The activity of an agent in obtaining, maintaining and terminating membership in one or more federations.</p> <p>Amplification: This activity also includes participation of federation members to negotiate policies and interface requirements for resource attribute management.</p>
Participate in Subject Attribute Federation	<p>The activity of an agent in obtaining, maintaining, and terminating membership in one or more subject attributes federations.</p> <p>Amplification: This activity also includes participation of federation members to negotiate policies and interface requirements for resource attribute management.</p>
Perform De-Installation	<p>The activity of an agent in removing managed objects from the technical infrastructure.</p> <p>Amplification: This activity includes the activities for doing the specification and completion of acceptance criteria for removal of IT infrastructure components prior to removal from the operational environment. This would include the removal of the MO's associated operational profiles and thresholds.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Perform Managed Object Shut Down	<p>The activity of an agent in shutting down a managed object in the GIG.</p> <p>Amplification: This activity performs the configuration management tasks necessary for the managed object (MO) to be successfully eliminated from the technical infrastructure without causing secondary or sympathetic service interruptions. This activity includes updating other supporting activities related to the MOs de-activation and elimination from the technical infrastructure. This activity prepares the MO for the de-installation activity.</p>
Plan Response to Situation	<p>The activity of an agent in (1) identifying response options, (2) analyzing response options, (3) selecting response, and (4) coordinating selected response.</p> <p>Amplification: This activity considers the overall assessment of the GIG (threats, vulnerabilities, incidents, and day-to-day needs).</p>
Prioritize Information Delivery	<p>The activity of an agent in prioritizing the delivery of information.</p> <p>Amplification: This function takes as its input an information flow precedence tag (e.g., routine, priority, emergency, survival, or planning) and returns a service ordering the overall set of information flows pending action. This ordering is based upon policy rule sets and may be established through various queuing protocols.</p>
Process Bandwidth Allocation and Response Requests	<p>The activity of an agent in processing bandwidth allocation and response requests.</p> <p>Amplification: All designated Global Information Grid NM Systems shall be capable of transmitting and receiving commonly formatted bandwidth allocation and access requests and responses that have been multiplexed with data traffic and carried in common physical, link, and network layers (though not virtual). GIG Network managers shall implement a bandwidth allocation function having a hierarchical structure with a single root node.</p>
Process Situational Awareness Data	<p>The activity of an agent in (1) detecting relevant SA events, (2) filtering SA Data, (3) correlating SA Data, (4) fusing SA data, and (5) categorizing SA data.</p> <p>Amplification: Data regarding the condition of information assurance, network operations, network management, and other GIG operations comprise situational awareness data. The data processed in this activity comprises security critical network and mission information that is used to build user-defined views of SA information. It includes the aggregation and formulation of data and information into associated reports and products.</p>
Provide Access	<p>The activity of an agent in controlling access to satellite communications channels.</p>
Provide Audit Reports	<p>The activity of an agent in reporting security-relevant information obtained through an examination of an audit trail.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Provide Communities of Interest	<p>The activity of a user in (1) identifying a COI with a similar mission, (2) establishing a COI if none currently exists with a similar mission, (3) managing the COI in accordance with the mission, and (4) participating in a COI to ensure its success.</p> <p>Amplification: Communities of Interest (COI) are established to promote net-centric information sharing. Communities provide an organization and maintenance construct for information such that the goals of the Data Strategy can be achieved. Establishing these activities at the COI level reduces the coordination effort necessary as compared to managing every data element Department-wide. DoDD 8320.2 directs that Domains within each of the Mission Areas (Business, Warfighter, Intel, and EIE) promote Net-Centric Information sharing and effectively enable COIs. When a Community of Interest (COI) is established through a Domain, the Domain portfolio management process will ensure resources are allocated to support the COI activities. COIs that form without being directed by a Domain will align themselves with an appropriate Domain(s) to leverage the capabilities provided by Domains. Once established, COIs should begin the activities identified in "Identify Information Assets." Communities should strive to bring the maximum visibility to the maximum number of assets as early as possible to support the DCIO tenet of "populating the network with new, dynamic sources of information to defeat the enemy." Concurrently, COIs should work to "Develop Semantic and Structural Information Agreements" for information sharing. While the Data Strategy goals of understandability and interoperability are heavily dependent on this activity, a significant amount of time may be needed to achieve these types of agreements. Therefore, COIs should not postpone making their information assets visible and accessible until this activity is completed. For more information on this activity see ""Develop Semantic and Structural Information Agreements."</p>
Provide Delivery Notification	<p>The activity of an agent in providing delivery notification for information products.</p> <p>Amplification: IDM will provide the capability for receivers of survival information to be notified by audio and visual alarms and the receivers of planning information to be notified based on user preference. May also include notification of delivery of Services.</p>
Provide Enterprise Information Catalog	<p>The activity of an agent in creating catalogs of information products and product updates.</p> <p>Amplification: IDM will provide the capability for information providers to automatically build information catalogs based on available information products and user profiles. Information providers should use standardized labels to describe their information and post the information to the catalog as soon as possible.</p>
Provide Information Awareness	<p>The activity of an agent in 1) providing smart push and pull capability, 2) providing enterprise information catalogs, 3) advertising catalog, 4) providing search and retrieval services, and 5) managing information flow.</p> <p>Amplification: The combination of these activities provides information consumers with an awareness of available information.</p>
Provide Key Ordering	<p>The activity of an agent in providing the ability to order cryptographic material based on mission needs.</p> <p>Amplification: This activity includes order validation activities.</p>
Provide Search and Retrieval	<p>The activity of an agent in allowing consumers to look for, locate and get desired information and services.</p> <p>Amplification: The search results are based on the set of information and service descriptions that are hosted by IDM. Information and service elements can be pulled on demand through the query of stored data using a search mechanism, or be periodically pushed to a consumer based on the consumer's profile.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definition
Provide Situational Awareness Data	<p>The activity of an authorized user or agent in making SA information and data visible and accessible to authorized users.</p> <p>Amplification: Data regarding the condition of information assurance, network operations, network management, and other GIG operations comprise situational awareness data. This activity is performed with the 'Share Information' set of activities in the 'Use the GIG' model. The SA data provided includes SA reports and products (UDOP, etc.), planned outages, violations, cyber attacks, anomalies, discrepancies, disruptions, and degradations.</p>
Provide Smart Push and Pull Capability	<p>The activity of an agent in providing a capability for information providers to disseminate information to specific consumers based on consumer established parameters.</p> <p>Amplification: This capability may be based on a subscription service, a consumer's profile, some other means, or a mixture of the three. Smart Push is defined as a transfer of information product(s) to information user(s) in response to profile(s) submitted (typically by the commander's staff) in anticipation of a group of information needs.</p>
Receive/Retrieve Situational Awareness Data from Audit Operations	<p>The activity of an agent in receiving or retrieving SA data and reports from audit operations.</p>
Recover GIG Resources	<p>The activity of an agent in (1) performing managed object shutdown, (2) performing de-installation, and (3) returning resources to inventory.</p>
Register Identity	<p>The activity of an agent in registering an identity of an entity.</p> <p>Amplification: Registering a GIG identity for an entity involves acquiring identity information from the entity, a sponsor for the entity and/or other sources.</p>
Respond to Situation	<p>The activity of an agent in (1) directing response, (2) executing response, and (3) maintaining optimal GIG performance.</p>
Retrieve Situational Awareness Data from Sensors	<p>The activity of an agent in retrieving required SA data from sensors and making it available to others.</p>
Return Resources to Inventory	<p>The activity of an agent in returning resources to inventory in an orderly, systematic process.</p>
Select Response	<p>The activity of an agent in evaluating the potential responses and selecting the best response for the given situation.</p> <p>Amplification: The selected response should resolve or escalate (i.e. referral to higher authority) any situation that is not part of the standard operation of the GIG and that causes, or may cause, an interruption to, or a reduction in, the quality of the GIG. The goal is to maintain and restore normal operations as quickly as possible and minimize adverse impacts to operations.</p>
Track and Account for Key	<p>The activity of an agent in tracking and accounting for cryptographic material throughout its lifecycle.</p>

NCOW RM v1.2 Activity Definitions

USE THE GLOBAL INFORMATION GRID (GIG)

Activity Name	Activity Definitions
Access Information	The activity of an authorized user in (1) locating an information asset, (2) connecting to an information asset, (3) acquiring an information asset access methodology, (4) acquiring an information asset access authorization, and (5) verifying the information asset's source and integrity.
Access Services	The activity of an agent in (1) locating a service, (2) connecting to the service, (3) negotiating with the service, (4) authenticating the service requester, (5) authenticating the requested service, and (6) acquiring access authorization to the service.
Access the Global Information Grid (GIG)	<p>The activity of a user in (1) activating a device that will be used to connect to the GIG, (2) logging into the GIG, and (3) establishing an authorized role.</p> <p>Amplification: This intermediate activity's subordinate leaf activities, when arrayed in a process thread, will require IA support (e.g., trusted path, identity management services, authentication services, certificate management services, token management services, biometric management services, the login service, access control services (e.g., device entry access control, network entry access control, service access control, data access control, and role-based access control, delegation of authority, least privilege control), and audit services).</p>
Acquire Access Authorization to the Service	<p>The activity of an access control service in (1) authorizing access to a requested service, and (2) the activity of an access control policy service in enforcing an authorization decision.</p> <p>Amplification: Access control makes and enforces decisions to control access to information, services, and resources based on policy, identity, environment, and resources. The authenticated invoking service and authenticated user must satisfy the service access control policy of the invoked service. This act completes the binding of the service.</p>
Acquire an Information Access Authorization	The activity of an authorized user in (1) providing needed inputs for access authorization decision, and the GIG system in (2) authorizing access to information and (3) enforcing the information authorization decision.
Acquire an Information Access Methodology	<p>The activity of an authorized user in obtaining the method needed to access the information asset.</p> <p>Amplification: For example, information assets may be accessed in a DBMS through SGL queries, stored procedures, data mining algorithms, etc.</p>
Acquire GIG Resources	The activity of an authorized user in acquiring the resources required to perform the operational activities associated with the user's role.
Acquire Metadata Dictionary	Describes non-contextual information about content, focusing on elements such as size, location or date of document creation providing little or no contextual understanding of what the document says or implies. This level of metadata is often the extent of many content management technologies.
Acquire Role-based Services	The activity of an authorized user in acquiring the services required to perform the operational activities associated with the user's role.
Activate Device	<p>The activity of a registered user in activating a device that will be used to establish a connection path between the user and the GIG.</p> <p>Amplification: For example, a user turns on a desktop computer that is "hard-wired" to the GIG, or a user takes the necessary action to initiate a login session with the GIG from a kiosk.</p>
Analyze and Confirm Protection Requirements	The activity of a protection service in analyzing the requirements of the protection invocation to ensure complete application of the required protections.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Assign COI-Specific Metadata Values	<p>The activity of an authorized user in assigning DDMS-compliant COI-specific metadata descriptors to an information asset.</p> <p>Amplification: Users assign metadata that is specifically COI content-related to their information asset. In order to discover information assets by COI subject matter, metadata values need to be assigned to the information asset. These values are developed and defined in the "Develop Semantic and Structural Information Agreements" activity as extensions and new tags. In this activity, users apply or assign the actual COI specific metadata values to an information asset that will then be registered (the metadata not the asset).</p>
Assign Discovery Metadata Values	<p>The activity of an authorized user in (1) assigning security metadata descriptors to an information asset, (2) assigning resource metadata descriptors to an information asset, (3) assigning summary content metadata descriptors to an information asset, and (4) assigning format metadata descriptors to an information asset.</p> <p>Amplification: Discovery metadata should comply with the DoD Discovery Metadata Specification (DDMS) and include associated structural metadata to support understandability. Automated processes should be used, whenever possible, to generate discovery metadata.</p>
Assign Format Metadata Descriptors	<p>The activity of an authorized user in assigning DDMS-compliant format metadata descriptors to an information asset.</p> <p>Amplification: DDMS compliant format metadata descriptors provide the description of physical attributes of the asset and include elements such as file size, bit-rate or frame-rate, and mime type. Automated processes should be used, whenever possible, to generate discovery metadata.</p>
Assign Metadata Values	<p>The activity of an authorized user in assigning (1) discovery metadata descriptors, (2) protection metadata descriptors, and/or (3) COI-specific metadata descriptor to an information asset.</p> <p>Amplification: The functions required to assign metadata values may be provided via a service.</p>
Assign Protection Metadata Values	<p>The activity of an authorized user in assigning protection metadata descriptors to an information asset.</p> <p>Amplification: This capability applies or assigns protection metadata to an information asset in order to place parameters around the protection of privacy, intellectual property, and/or any other special restrictions or limitations.</p>
Assign Resource Metadata Descriptors	<p>The activity of an authorized user in assigning DDMS-compliant resource metadata descriptors to an information asset.</p> <p>Amplification: DDMS-compliant resource metadata descriptors describe aspects of an information asset that support maintenance, administration, and pedigree of the information asset. Automated processes should be used, whenever possible, to generate discovery metadata.</p>
Assign Security Metadata Descriptors	<p>The activity of an authorized user in assigning DDMS-compliant security classification and related metadata descriptors to an information asset.</p> <p>Amplification: These fields provide for the specification of security-related attributes and may be used to support access control. The security set is intended to support comprehensive resource security markings as prescribed by CAPCO. To accomplish this, the DDMS refers to the IC ISM implementation of the CAPCO standards. For communities for which IC ISM does not suffice, additional security elements may be represented using the metadata elements defined by organizations and COIs, and stored in the Extensible Layer (see "Generate COI-Specific Metadata Descriptors"). See Intelligence Community Metadata Standards for Information Assurance, "Information Security Marking Data Element Dictionary." See also, Intelligence Community Metadata Standards for Information Assurance, "Information Security Marking Implementation Guide" for the complete set of security attributes. Automated processes should be used, whenever possible, to generate discovery metadata.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Assign Summary Content Metadata Descriptors	<p>The activity of an authorized user in assigning DDMS-compliant summary content metadata descriptors to an information asset.</p> <p>Amplification: DDMS- compliant summary content descriptors specify concepts and additional contextual aspects of the information asset such as subject, description, and coverage. These elements are intended to capture information asset-level information that describes the content and/or context. This set of descriptors is intended to aid in precision discovery and to offer a level of description above standard indexing. Developed ontologies (vocabularies, taxonomies) should be utilized in describing information assets to ensure they are described in a consistent way across the community. Information on developing ontologies can be found in activity "Define Ontologies". Automated processes should be used, whenever possible, to generate discovery metadata.</p>
Associate Metadata to an Information Asset	<p>The activity of an authorized user in (1) assigning metadata values to an information asset, and (2) binding metadata to an information asset.</p> <p>Amplification: Metadata is applied to information assets, be they data or services. The functions required to associate metadata may be provided via a service.</p>
Authenticate a Requested Service	<p>The activity of an agent in (1) validating the authentication request of a requested service, (2) verifying the credentials of the requested service, and (3) making an authentication decision for the requested service.</p>
Authenticate a Service Requester	<p>The activity of an agent (1) validating the authentication request of the service requester, (2) verifying the credentials of the service requester, and (3) making an authentication decision for the service requester.</p>
Authenticate a Service User	<p>The activity of an authentication service in (1) validating the authentication request of the service requester, (2) verifying the credentials of the service requester, and (3) making an authentication decision for the service requester.</p>
Authorize Access to a Service	<p>The activity of an access control service in (1) retrieving and validating input needed to make an authorization decision, (2) evaluating the inputs with respect to the appropriate access policy and making an authorization decision in regard to the service requester, and (3) distributing the authorization decision.</p> <p>Amplification: This activity includes locating and evaluating applicable authorization policy, and making the authorization decision, which requires the retrieval and validation of inputs relevant to the specific access request including: requester authentication information, requested action type, requester attributes, service attributes, and environmental factors. Evaluating policy rules may require the determination of values for operational need, security risk, and requester heuristics. Making the authorization decision may require the determination of constraints and obligations. The authorization decision must be distributed as appropriate for enforcement, father endorsement, and/or requester notification.</p>
Authorize Access to Information	<p>The activity of an access control policy service in (1) retrieving and validating input needed to make an authorization decision, (2) evaluating the inputs with respect to the appropriate access policy and making an authorization decision in regard to the information asset requester, and (3) distributing the authorization decision.</p>
Bind Metadata to Information Asset	<p>The activity of an authorized user in binding DDMS-compliant metadata to an information asset.</p> <p>Amplification: Once discovered, binding enables metadata to align strictly with its information asset. This capability allows the user to bind the metadata in a tight coupling with its information asset in order to avoid any metadata being associated with information assets other than its own. The required functions for binding metadata may be provided via a service.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Canonicalize Data	<p>The activity of a trusted user in converting (as necessary) the information asset to a standard format.</p> <p>Amplification: This activity does not destroy or modify any of the information content. Canonicalization is used for the purpose of converting to a standard format suitable for inspection or for sanitization. The canonicalized information may be returned to the Review activity for reinspection.</p>
Connect to Information	The activity of an authorized user in connecting to the information asset.
Connect to Service	<p>The activity of an agent in accessing the interface of a service.</p> <p>Amplification: Involves the acts of packaging the service request into a message, and executing the service messaging protocol to resolve (traverse) the connection path to gain the capability to interact with the invoked service's interface.</p>
Discover Information	<p>The activity of an authorized user in discovering information by searching federated metadata catalogs for desired information.</p> <p>Amplification: The discovery metadata for each information asset is catalogued so that the asset may be found through an enterprise search. Note that information is accessed while a service is used.</p>
Discover Information Asset	<p>The activity of an authorized user in (1) discovering information to be accessed and (2) discovering services to be used.</p> <p>Amplification: Discovered Information assets could include, but is not limited to, information, services, information sources (e.g., databases), COIs, semantic metadata and/or structural metadata. Information assets are discoverable by any of the DDMS core or extended fields across the Enterprise. Discovered information assets should indicate its availability as not all visible information assets are accessible and indicate whether it is the authoritative source (see "Define Authoritative Sources").</p>
Discover Services	<p>The activity of an authorized user in discovering a service by searching federated service registries to be used by the user.</p> <p>Amplification: The discovery metadata for each service is catalogued so that the asset may be found through an enterprise search. Note that a service is used while information is accessed.</p>
Distribute the Authorization Decision	The activity of an access control policy service in distributing the authorization decision to the access control enforcement service.
Enable Capability Interface	The activity of an agent in making a capability interface functional with the information, services, and resources required for an authorized user to perform the operational activities associated with the user's role.
Enforce Service Authorization Decision	The activity of an access control enforcement service in (1) retrieving and validating authorization decision parameters, and (2) invoking protection services to meet constraints and obligations.
Enforce the Information Authorization Decision	The activity of an access control enforcement service in (1) retrieving and validating authorization parameters, and (2) invoking protections that satisfy any required constraints and obligations.
Establish Authorized Role	The activity of an authenticated user in providing the role information required by a policy-enforcement mechanism to control use of the GIG.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Establish Capability Interface	<p>The activity of an authorized user in (1) acquiring role-based services, (2) acquiring GIG resources, and (3) enabling a capability interface.</p> <p>Amplification: The services and resources provided are based on the user role.</p>
Evaluate Policy Rules	<p>The activity of an access control policy service in evaluating inputs (relevant attributes of the requested service and relevant attributes of the service requester) with respect to the appropriate access policy and deciding whether access to a resource should be granted.</p> <p>Amplification: This evaluation is governed by overarching policies that dictate how the authorization decision is reached (e.g. least privilege) and includes identification and specification of constraints and obligations required for access to the requested information.</p>
Interact Through Capability Interface	<p>The activity of a registered user in (1) accessing the GIG, (2) establishing a capability interface, and (3) using a capability interface.</p> <p>Amplification: This intermediate activity establishes the basis for interacting with the GIG. It addresses an NCOW RM abstraction for a Capability Interface that encapsulates the operational user's role and enables that user to interact with the GIG in acquiring and using services to create and manipulate data assets. The implementation details of this interface depend upon the device on which it is implemented, the displays needed, the interactive capability needed, and human-computer interface design decisions. For example, a user turns on a desktop computer that is "hard-wired" to the GIG, or a user takes the necessary action to initiate a login session with the GIG from a kiosk.</p>
Interact with Allocated Resources	<p>The activity of an authorized user in interacting with and using resources allocated to the user via a capability interface for the user to perform the operational activities associated with the user's role.</p>
Interact with Information	<p>The activity of an authorized user in (1) requesting information and (2) using information to perform the operational activities associated with the user's role.</p> <p>Amplification: Once information is requested, access to the information must be provided before it can be used.</p>
Interact with Services	<p>The activity of an authorized user in (1) requesting services and (2) using services to perform the operational activities associated with the user's role.</p> <p>Amplification: Once a service is requested, access to the service must be provided before it can be used.</p>
Invoke Protections to Meet Constraints and Obligations	<p>The activity of an access control enforcement service in invoking protection services required to meet the constraints and obligations of an authorization decision.</p> <p>Amplification: The protections are invoked to ensure that specified qualities of protection (QoP) are achieved end-to-end for all transactions.</p>
Locate Information	<p>The activity of an authorized user in selecting upon discovery, or obtaining directly the location of an information asset.</p>
Locate Service	<p>The activity of an agent in obtaining the location of the interface to a service.</p> <p>Amplification: Service interface locations may be locally cached and directly obtainable without having to use a discovery service.</p>
Login to Global Information Grid (GIG)	<p>The activity of a registered user in providing the identity and authentication information required by a policy-enforcement mechanism to authorize access to the GIG.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Make Authentication Decision for a Requested Service	<p>The activity of an authentication service in deciding on the validity of a requested service's credential(s) and distributing the resulting decision.</p> <p>Amplification: This activity includes determining and reporting achieved authentication assurance level.</p>
Make Authentication Decision for Service Requester	<p>The activity of an authentication service in deciding on the validity of a service requester's credential(s) and distributing the resulting decision.</p> <p>Amplification: This activity includes determining and reporting achieved authentication assurance level.</p>
Negotiate with Service	<p>The activity of an agent in (1) identifying the parameters applicable to a service agreement with the service, (2) establishing a service agreement to be used in binding to the service, (3) binding to the service, and (4) using that service.</p>
Place Information in Accessible Storage Mechanism	<p>The activity of an authorized user in placing the information asset into an accessible storage mechanism.</p>
Post COI-Specific Metadata	<p>The activity of an authorized user in providing COI-specific metadata for an information asset to federated COI-specific discovery catalogs.</p>
Post Discovery Metadata	<p>The activity of an authorized user in providing discovery metadata for an information asset to federated discovery catalogs.</p> <p>Amplification: An enterprise federated discovery catalog is any mechanism, which can be searched to determine the existence of information assets, and which implements the DoD Discovery Interface Specification for enterprise discovery. Providing discovery metadata to these types of catalogs supports the visibility of information assets throughout the enterprise.</p>
Post Information Asset	<p>The activity of an authorized user, or a service acting on the user's behalf, in (1) posting an information asset, and (2) posting the metadata of the information asset.</p> <p>Amplification: If the capability does not currently exist to ensure Information Assets are accessible in the GIG, these capabilities should be provided in the "Evolve the GIG" model. Information Assets should be accessible by all users, when and where needed in the DoD, except where limited by law, policy, or security classification. In addition, accessible Information assets should conform to DoD-specified data publication methods and not require specialize applications or vendor licenses.</p>
Post Information to the GIG	<p>The activity of an authorized user in (1) selecting an accessible storage mechanism, and (2) placing the information asset into the accessible storage mechanism.</p> <p>Amplification: Information assets should be accessible by all users, when and where needed in the DoD, except where limited by law, policy, or security classification. In addition, accessible information assets should conform to DoD-specified data publication methods and not require specialized applications or vendor licenses.</p>
Post Metadata to the GIG	<p>The activity of an authorized user in (1) posting discovery metadata for an information asset, (2) posting protection metadata for an information asset, and (3) posting COI-specific metadata for an information asset.</p>
Post Protection Metadata	<p>The activity of an authorized user in providing protection metadata for an information asset to federated protection catalogs.</p>
Prepare Information for Sharing Across Security Domains	<p>The activity of a trusted user in (1) reviewing an information asset in the context of appropriate cross domain sharing security policy, (2) canonicalize the information asset, (3) sanitize the information asset, and (4) regrade the information asset, as necessary, prior to allowing it to cross a domain boundary.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Protect a Resource	The activity of protection services in (1) analyzing and confirming protection requirements, (2) providing confidentiality, (3) providing integrity, (4) supporting availability, and (5) providing non-repudiation.
Provide Confidentiality	<p>The activity of a confidentiality service in ensuring appropriate services are applied to meet the confidentiality requirements of the given information or transaction.</p> <p>Amplification: Confidentiality may be achieved by providing controlled access and controlled information flow. Non-access control related confidentiality services include cryptographic services for encrypting and decrypting information and the employment of COMSEC and TRANSEC mechanisms as appropriate for all components actively protecting GIG communications paths.</p>
Provide Integrity	The activity of an integrity service in ensuring that appropriate services are applied to meet the integrity requirements of the given information or transaction.
Provide Non-repudiation	The activity of a non-repudiation service in collecting, creating, and providing evidence that confirms the participation of parties in a transaction.
Regrade Information	<p>The activity of a trusted user in regrading the information asset.</p> <p>Amplification: Regrading usually happens after a sanitization activity has occurred to create a new information asset based on the specific transaction constraints and cross-domain sharing security policy. Note that regrading could also occur when an information asset is declassified without previous sanitization.</p>
Request Information	<p>The activity of an authorized user in requesting the information required to enable that user to perform the operational activities associated with the user's role.</p> <p>Amplification: The user will request information through a service that is active at the Capability Interface.</p>
Request Services	<p>The activity of an authorized user in requesting services required to enable that user to perform the operational activities associated with the user's role.</p> <p>Amplification: Everything that occurs in the GIG will happen via a selected or specified service. Once requested, several activities occur to provide access to the service.</p>
Retrieve and Validate Authorization Decision Parameters	The activity of an access control enforcement service in retrieving and validating authorization parameters against the authorization decision.
Retrieve and Validate Needed Inputs	The activity of an access control policy service in retrieving and validating environment parameters needed to make an authorization decision.
Review Information	<p>The activity of a trusted user in inspecting an information asset in terms of a defined information asset sharing security policy.</p> <p>Amplification: This review is in the context of sharing information across security domains. Examples of information review actions include:</p> <ul style="list-style-type: none"> - Identify Object Data Type - Inspect for Malicious Code - Context-based Content Inspection - Validate Appropriateness of Metadata - Analyze for Covert Channels - Provide Human Review <p>Based on the review, requirements are generated for canonicalization, sanitization, and regrading.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Sanitize Information	<p>The activity of a trusted user in sanitizing (as necessary) the information asset.</p> <p>Amplification: This is an active process that can make destructive changes to the content of an information asset. The Review Activity identified the existence of elements that violated the cross domain sharing security policy; whereas the sanitization activity modifies, or cleans, the information asset based on the disposition rules defined in the cross domain sharing security policy.</p>
Select Accessible Storage Mechanism	<p>The activity of an authorized user in selecting an accessible storage mechanism for an information asset.</p> <p>Amplification: An accessible storage mechanism is any storage medium that allows authorized access to its information. This medium may be managed and offered at a local, regional or global level.</p>
Share Information	<p>The activity of an authorized user in (1) associating metadata to an information asset, (2) posting the information asset, (3) preparing an information asset for sharing across security domains, (4) discovering an information asset, (5) accessing an information asset, and (6) understanding an information asset.</p> <p>Amplification: Users share information by making data visible, accessible, and understandable to other users in the GIG using available GIG capabilities (e.g., information sharing service). Users providing data to the GIG describe the data with DDMS compliant discovery metadata, associate structural metadata, provide discovery metadata to enterprise federated discovery catalogs, and ensure data can be accessed from the GIG. Information sharing capabilities for users providing data to the GIG is supported by data strategy activities described in the "Evolve the GIG" model. (e.g., "Provide Data Services"). Understandability is supported by associating semantic and structural metadata to provided data (development of semantic and structural metadata is described in "Evolve the GIG"). Users discover access and understand information assets in the GIG using available GIG capabilities. Together, these capabilities result in the overall capability to share information.</p>
Support Availability	<p>The activity of an availability support service in ensuring that appropriate services and resources required to provide information availability (e.g., fault tolerance, survivability, performance quality) exist and are applied to meet the availability requirements of the given information and transaction.</p>
Understand Information Asset	<p>The activity of an authorized user in understanding information or a service's capabilities by virtue of the semantic metadata of the information or service.</p> <p>Amplification: This context may be the underlying structure, pedigree, vocabulary, timeliness, or other metadata information, which facilitates user needs. This capability comes from both the ability to view the discovery metadata for a given asset and to access the associated semantic and structural metadata. Metadata for an asset should be readily available for discovered and accessed information assets, and should not require an additional discovery process (i.e., semantic and structural metadata locations for a given information asset should be associated with its discovery metadata). All metadata in this activity (i.e., discovery, semantic and structural) has been previously defined by information owners.</p>
Use Information	<p>The activity of an authorized user in using information necessary for that user to perform the operational activities associated with the user's role.</p> <p>Amplification: The purpose of this activity is to convey the need for the user to gain/provide value by using the information that is made available through the CI.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Use Capability Interface	<p>The activity of an authorized user in (1) interacting with services, (2) interacting with information, and (3) interacting with allocated resources.</p> <p>Amplification: The capability interface encapsulates a role (i.e., it contains the set of services and/or a service orchestrator needed to perform that role). Services are invoked or requested through the capability interface. Services may request other services. Allocated resources support this use of services.</p>
Use Services	<p>The activity of an authorized user in using services to conduct assigned tasks and missions.</p> <p>Amplification: Prior to using a service, the service is requested and access to the service is provided.</p>
Use the Global Information Grid (GIG)	<p>The activity of a registered user in (1) interacting with the GIG through a capability interface, (2) accessing services, (3) protecting resources, and (4) sharing information.</p> <p>Amplification: This top-level activity establishes that all users will use the Net-Centric Environment of the GIG in performing their operations. Includes actions to access the GIG, establish and use a capability interface, access services, provide information, and access information.</p>
Validate Authentication Request of Service Requester	<p>The activity of an authentication service in validating the attributes of the authentication request.</p> <p>Amplification: Includes looking up and retrieving credentials and attributes that may not be included in the original request and ensuring that identifiers refer to valid identities. The attributes and credentials are passed to later activities in fulfillment of the authentication request.</p>
Validate the Authentication Request of a Requested Service	<p>The activity of an authentication service in validating the attributes of the authentication request.</p> <p>Amplification: Includes looking up and retrieving credentials and attributes that may not be included in the original request and ensuring that identifiers refer to valid identities. The attributes and credentials are passed to later activities in fulfillment of the authentication request.</p>
Verify Data Source and Integrity	<p>The activity of an access control service in verifying the source (the actual source is the same as the claimed source) and the integrity of the asset has not been modified) of an information asset.</p>
Verify the Credentials of a Requested Service	<p>The activity of an authentication service in deciding on the validity of a requested service's credential(s) based on attributes of the authentication request.</p> <p>Amplification: This action may occur through services provided by a third party (e.g., OSCP).</p>
Verify the Credentials of the Service Requester	<p>The activity of an authentication service acting on behalf of a service requester in determining the validity of a service requester's credential(s) based upon the attributes of the authentication request.</p> <p>Amplification: This action may occur through services provided by a third party (e.g., OSCP).</p>

NCOW RM v1.2 Activity Definitions

EVOLVE THE GLOBAL INFORMATION GRID (GIG)

Activity Name	Activity Definitions
Accredit Integrated Capability for Operation	This activity provides the approval to operate a newly integrated increment of GIG capability. It is performed by a designated accreditation authority and uses increment and increment integration certification information as the basis for approval.
Advance Computing Infrastructure Technology	This activity involves providing computing services that are able to be shared across the DoD Enterprise such as Grid computing applications, virtual computing applications, and support for collaborative applications. Services are provided by the grid, service-oriented, and collaborative CI environments. Note: This activity was identified as a tentative activity for incorporation into a future version of the NCOW RM.
Apply Internet Standards	No single country or organization is responsible for setting Internet conventions. The organizations that participate in setting Internet standards and the relationships are divided among organizations according to the type of standards they help define: technical specifications (for example, what type of fields are required in an IP datagram) and addressing and domain name policies (for example, who owns rights to post files to a Web page located at www.course.com).
Apply Set of Standards	To use a standard or set of standards in support of a capability or need in the net-centric environment.
Apply Telecommunications Industry Standards	The telecommunications industry is guided by standards prescribed by many national and international organizations. Standards are documented agreements containing technical specifications or other precise criteria that stipulate how a particular product or service should be designed or performed. Example of organizations, ANSI, TIA, EIA, IEEE, ATIS ISO, ITU.
Architect Assurance Capabilities	To plan and describe the capabilities required to assure all information and network related activities in the net-centric environment. These capabilities are reflected in a set of core, common, and mission-specific services.
Architect Data Networks Infrastructure	The use of electrical signals to exchange encoded information between computerized devices across a distance.
Architect Enterprise Services Capabilities	To plan and describe the service capabilities that is essential for conducting operations in a net-centric environment. These capabilities are reflected in a set of core, common, and mission-specific services.
Architect Global Information Grid (GIG) Capabilities	To plan and describe key elements of the IT infrastructure, capabilities, and technologies needed to achieve a net-centric environment. This activity uses inputs from provided guidance and direction, and considers existing infrastructure, capabilities, and technologies.
Architect Net-Centric Environment Infrastructure	To plan and describe the integrated infrastructure required to support and enable the GIG. The description should address the transport, computing, data, and assurance (IA/NetOps) infrastructures as a minimum.
Architect Net-Centric Information Capabilities	To plan and describe the information capabilities required to support and enable operations in the net-centric environment. This activity establishes the service-oriented approach, and addresses all aspects of core services and other required services.
Architect Supporting Technologies	To plan and describe the technologies required to realize the infrastructure, services, and processes associated with the net-centric environment. These technologies may become DoD standards.
Architect Telephone Networks Infrastructure	- PSTN (public switched telephone network) is the world's collection of interconnected voice-oriented public telephone networks, both commercial and government-owned.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Architect the Assurance Infrastructure	To plan and describe the assurance infrastructure required to support and enable assurance of the GIG. The assurance infrastructure includes information assurance (IA) and network operations (NetOps) infrastructures, and establishes the foundation for all net-centric assurance related operations.
Architect the Communications Infrastructure	
Architect the Computing Infrastructure	To plan and describe the computing infrastructure required to support and enable the GIG. The computing infrastructure establishes the foundation for all net-centric computing.
Architect the IA Infrastructure	To plan and describe the information assurance (IA) infrastructure required to support and enable assurance of the GIG. The IA infrastructure, along with the NetOps infrastructure, establishes the foundation for all net-centric assurance related operations.
Architect the NetOps Infrastructure	To plan and describe the network operations (NetOps) infrastructure required to support and enable assurance of the GIG. The NetOps infrastructure, along with the IA infrastructure, establishes the foundation for all net-centric assurance related operations.
Architect the Transport Infrastructure	To plan and describe the transport infrastructure required to support and enable the Global Information Grid (GIG). The transport infrastructure establishes the foundation for all forms of net-centric communications.
Assess Readiness for Increment Integration	This activity takes a given increment of EIE capability and analyzes and evaluates its inherent performance and assurance prior to integration. It tests all relevant interfaces that enable the integration to ensure they can integrate successfully. The results of this assessment are subsequently used in certifying the fully integrated capability.
Assign Network Responsibilities	Determine and allocate responsibility to appropriate entities for various aspects of networks within the GIG.
Assign Responsibilities for Integrating Functions	Determine and allocate responsibility for integrating functions to appropriate entities.
Assign Specific Responsibilities within Assigned Boundaries	Give entity specific responsibilities within the specifically established area of the GIG.
Certify Integrated Capability	To confirm an integrated capability performs as expected. This addresses all aspects of the capability to include functionality and supporting elements. It is performed by a designated certification authority.
Complete Certification Application Forms	This activity is performed to obtain the frequency assignments for system equipment so that it can operate at that particular frequency band. Source: Department of Commerce, Office of Radio Frequency Management
Conduct Attack/Event Response	The ability to ensure timely detection and appropriate response to attacks and events that impact the GIG. Amplification: This capability includes enterprise-wide monitoring and detection of inappropriate activities and matches the correct response to the threat.
Conduct Engineering Analysis and Calculations	This activity is needed for a variety of uses, including converting coordinates from one form to another, developing topographical charts of signal coverage, determining the necessary satellite look-angles of ground stations, performing HF sky wave propagation, performing link analysis calculations, and drawing spectrum-occupancy graphs for frequency bands. Source: Department of Commerce, Office of Radio Frequency Management
Conduct NetOps Reporting	Enabling CI resources to continually report status to NetOps.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Conduct Research and Development Efforts	This activity encompasses the Research and Development necessary to develop and evolve innovative technology solutions to advance DoD CI capabilities.
Control Capability Increment Integration	This activity aggregates the functions of managing all aspects of integrating a new increment of capability within the information environment. Key aspects of control include timing, funding, readiness for implementation, and post-implementation assessments. The input to this activity is the notification for a new capability to be integrated into the information environment and its state of development. Timing of this activity may be made coincident with capability assessments or program milestones. This activity could be as simple as introducing a new application or as complex as introducing a transformational communications capability. GIG governance activities are included as sub-activities within this activity.
Coordinate Establishing Content and Content Mapping	This activity focuses on loading content and mapping that content at system initialization/re-initialization. It is coordinated by NetOps Content Managers and performed by NetOps Administrators. It is controlled by the functions to be performed within the extended elements of the Global Information Grid (GIG), the storage resources available, and by standard Net-Centric operating procedures.
Coordinate Establishment of Logistics Support	Arrange for required operational and resource support to ensure logistical needs for network operations are met.
Coordinate Network Capability Planning and Engineering with Commercial Provider	This activity focuses on the process of gaining communications service-level agreements, standard net-centric operating procedures, and functional performance capabilities from networking operations that are to be provisioned by a Commercial Provider. This networking capability may be provisioned in the form of information transport over host-nation commercial facilities or through transport provisioned by a U.S. commercial provider. It is usually implemented through contractual arrangements or a service level agreement. It addresses the specific connections, transmission media, networking hardware and associated software to be installed and integrated into the Global Information Grid (GIG) as part of a new and/or evolving information transport capability. It includes defining, establishing, evolving, and integrating GIG networking functions in response to operational (mission) requirements. This activity may use auction services to fill peak demands in a more dynamic fashion. The inputs to this activity are GIG architecture information, desired networking operational capabilities, physical plant constraints, and computer and software resources. It provides new contracts, service-level agreements, updates to standard net-centric operating procedures, and installed information transport capabilities that can support operational needs. DoD policy, guidance, funding, contracts, GIG architectural governance, functional performance requirements, and communications engineering "best practices" provide controls to this activity.
Coordinate System Capability Engineering with Commercial Provider	This activity focuses on the process of gaining service-level agreements, standard net-centric operating procedures, and functional performance capabilities from computing operations that have been outsourced to a Commercial Provider (e.g., Navy Marine Corps Intranet [NMCI]). It addresses the specific computer hardware and associated software to be installed and integrated into the Global Information Grid (GIG) as part of a new and/or evolving functional capability. It includes defining, establishing, evolving, and integrating GIG computing functions in response to operational (mission) requirements. The inputs to this activity are GIG architecture information, physical plant constraints, and computer and software resources. It provides new service level agreements, updates to standard net-centric operating procedures, and installed computational capabilities that can support operational needs. DoD policy, guidance, funding, contracts, GIG architectural governance, functional performance requirements, and engineering best practices provide controls to this activity.
Coordinate Theater Broadcast Schedules	To arrange or consolidate Theater broadcast schedules for effectiveness and efficiency.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Define Administrative Domains, Authorities, and Responsibilities	This activity focuses on establishing the administrative boundaries within the Global Information Grid (GIG), identifying authorities to oversee and control actions within these boundaries, and assigning specific responsibilities to NetOps personnel within these boundaries as well as assigning cross-domain responsibilities and authorities. This activity includes defining the set of Trust Domains to be established within the enterprise information environment.
Define Authoritative Sources	Information asset owners (e.g. system owners, information producers, information management staff) participate in COIs identify the authoritative sources information assets. COIs may support information providers in resolving potentially conflicting sources and, where appropriate, coordinate with the DoD-wide governance bodies to identify authoritative source(s). The community should provide authoritative source metadata to the GIG, so users and applications can evaluate and understand the community-implied authority of information sources. This authoritative source metadata should be accessible when Users discover information assets (see "Discover Information Asset") to ensure Users are able to make informed decisions in accessing an information asset. Moreover, Users discovering and identifying a COI should be able to determine the authoritative information sources controlled or maintained by the Community. This is a sub-activity of "Identify Information Assets."
Define Common Information Models	Communities of Interest define common information models to facilitate the sharing of information within the community and to the Enterprise. This model provides a canonical data representation between multiple information sources and facilitates a shared understanding of the community's information. Common information models enable information integration for communities and reduce the requirement for point-to-point interfaces between information sources. Common Information models should be provided to the GIG in an enterprise federated metadata registry. This is a sub-activity under "Develop Semantic and Structural Information Agreements."
Define Content Staging Strategies, Policies, and Plans	This activity establishes current and future content-staging goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for content-staging infrastructure, operations, sustainment, and readiness.
Define Hierarchical Network Topology	This activity establishes the necessary tiers of subnets needed for communications support. For example, a single unit would need a local area network to support communications among all the users aboard the vessel, a task unit would need a metropolitan area network to interconnect all the single unit's local area subnetworks, and a strike group would need a wide area network to interconnect all the task unit's metropolitan subnetworks. Controls for this activity include geography, cost, considerations, and communities of interest among the users. Source: Communication Networks: Fundamental Concepts and Key Architectures, Leon-Garcia, 2000.
Define IA Strategies, Policies, and Plans	This activity establishes current and future IA goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for all aspects of IA.
Define Information Sharing Metrics	Information Sharing metrics are defined to measure and track implementation of the Net-Centric Data Strategy approaches. Measurement techniques should be developed to ensue that metrics are captured in a useful and consistent manner. Examples of data metrics include percent of web-enabled components, progress toward service-enabling identified key functional components and percent of tagged Community data. Information Sharing metrics should be "tagged" with DDMS compliant metadata and provided to the GIG to promote awareness of data management successes and areas requiring improvement.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Define Information Sharing Policies	Information sharing policies are developed that extends the guidance in DoDD 8320.2 and the concepts in the DoD Net-Centric Data Strategy. Policies should define responsibilities for the community members in clear and concise detail and should also include the identification of data goals and overarching vision for each community. These policies should include information asset publication policies to align community information with DoD publication policies. These information sharing policies are important for institutionalizing the DoD Net-Centric Data Strategy goals and concepts (e.g., tag information assets with DDMS, support Communities of Interest) within their community.
Define Interface Specifications	Interface specifications are defined for key interfaces identified by Communities of Interest. COIs should reference applicable Net-Centric Key Interface Profiles (KIPs), and align their identified interfaces as appropriate. Interface specification should be provided to the NCE through enterprise federated metadata registries to support cross-COI and Enterprise-wide interoperability. This is a sub-activity under "Develop Semantic and Structural Information Agreements."
Define Interoperability Specifications	Communities of Interest define interoperability specifications to specify the requirements for ensuring consistent and standardized data interchange, both within communities and Enterprise-wide. Specifications for interoperability will include identification of key interfaces, definitions for data sharing services and access layers, data model and schema for the shared data, and translation and transformation components. The COI will tag the interoperability specifications document with DDMS compliant metadata and provide it the GIG through a enterprise federated metadata registry (e.g., DoD Metadata Registry). Mediation services will use the registered metadata to facilitate system interoperability between unanticipated interfaces as needed. This is a sub-activity under "Develop Semantic and Structural Information Agreements."
Define NetOps Functions	Describe the set of functions associated with network operations.
Define NetOps Strategies, Policies, and Plans	This activity establishes current and future NetOps goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for all aspects of NetOps.
Define Network Demarcations, Authorities and Responsibilities	This activity establishes the boundaries of Global Information Grid (GIG) networks, gateways through which information import/export must occur and where external users must enter into GIG networks. The activity assigns network responsibilities and identifies authorities for executing oversight and control of assigned network responsibilities. Network demarcations may be established within the GIG to provide additional controls.
Define Ontologies	Communities of Interest develop an ontology that reflects understanding of its shared information. Ontologies include taxonomies, thesauri, vocabularies, and associations; promoting semantic and syntactic understanding of data (e.g. taxonomies enhance discovery by providing a hierarchical means of searching for data while providing users with additional insights about information assets by indicating their placement relative to other information assets). Semantic relationships between vocabulary terms should be defined to facilitate expansion of search and understanding capabilities. Ontologies should align to Enterprise-wide ontologies to ensure a shared understanding of information assets across the Enterprise. Communities can utilize ontologies in structuring catalogs, registries and directories. Additionally, information assets "tagged" with agreed upon, consistent terms (e.g., vocabulary, key words, taxonomy), facilitate discovery and understanding of information assets. Communities may also develop a thesaurus to associate words with similar meanings together. Ontologies should also be maintained and evolved with the environment (see "Manage Ontologies"). This is a sub-activity under "Develop Semantic and Structural Information Agreements."

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Define Service Levels	Service providers define and publish measurable service levels (e.g., Service Level Agreements) to the GIG. Users utilize this information to determine if services will provide the need level of service to support their specific mission. Service levels should reflect provided user feedback (see "Respond to User Feedback"). Service Levels should be provided to the GIG in an enterprise federated service registry. This is a sub-activity under "Provide Service."
Define Status Reporting Requirements	This activity focuses on the reporting requirements at various levels of NetOps management to ensure NetOps personnel can maintain Global Information Grid (GIG) situational awareness. Situational-awareness requirements, policy, guidance, monitoring capabilities, and standard NetOps operating procedures control this activity. NetOps personnel perform this activity. This activity takes desired situational awareness capabilities as inputs, and produces standardized NetOps status reporting procedures, an established reporting hierarchy, and identified authorities for overseeing and controlling NetOps reporting as outputs.
Define Systems and Network Management Strategies, Policies, and Plans	This activity establishes current and future systems and networks goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for all systems and networks modernization, operations, and sustainment including systems and networks portfolio investment management.
Define Translations and Transformations	Information providers and consumers define translations and mediation capabilities necessary for the shared information to be understandable and usable for both human and machine users. The translation capability should utilize the semantic data agreements (e.g., descriptions, vocabularies, taxonomies, thesauruses, key word lists) to ensure the information is understandable to the user. The transformation capability should apply the structural data agreements (e.g. format-related metadata, schemas, COI extension to DDMS, web service tags, access control metadata) to ensure the information is usable to the user. This is a sub-activity under "Develop Semantic and Structural Information Agreements."
Deliver Net-Centric Computing Infrastructure	Computing infrastructure in the net-centric environment will be customer-driven, shared, dynamically allocated, and automatically monitored and configured. Net-centric computing infrastructure will enable , location-independent storage; dynamic, automated storage provisioning, virtualized application environments, grid computing and automated status reporting .
Determine Host Nation Frequency Supportability	This activity is required for all frequency assignments, by all international telecommunications agencies, to evaluate future allocations of those assignments. Source: Navy-Marine Corps Spectrum Center (NMSC)
Determine Requirement for Tactical Reach-back	Establish the full set of capabilities required for tactical reach-back based on mission needs and other factors.
Develop and Test NCOE	This activity involves the development and testing of the net-centric operational environment (NCOE). The NCOE addresses the key enablers of the GIG core infrastructure; GIG-BE, JTRS, TSAT, NCES, GIG-IA, Teleport, and JNMS.
Develop and Test Tactical Reach-back	This activity coordinates the establishment of extensions of the Global Information Grid (GIG) communications backbone to tactical forces. It coordinates the establishment of Theater Injection Points and in coordinating and consolidating Theater broadcast schedules.
Develop Assurance Capabilities	To design, develop, and test those capabilities that support and enable assured networks and assured information. Includes NetOps and IA related capabilities.
Develop Assurance Strategies, Policies, and Plans	This activity establishes current and future assurance (NetOps and IA) goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for all aspects of assurance.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Develop Communications Strategies, Policies, and Plans	This activity establishes current and future communications goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for all communications modernization, operations, sustainment, and readiness including communications portfolio investment management.
Develop Computer Hardware and Software Installation	This activity focuses on the specific computer hardware and associated software to be installed and integrated into the Global Information Grid (GIG) as part of a new and/or evolving functional capability. The inputs to this activity are GIG architecture information, physical plant constraints, and computer and software resources. It provides computational capabilities, and installation integration plans that can support operational needs. Such engineering may include the design of anti-tamper and radiation hardened devices. DoD policy, guidance, funding, GIG architectural governance, functional performance requirements, and engineering best practices provide controls to this activity.
Develop Computing Strategies, Policies and Plans	This activity establishes current and future computing goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for all computing modernization, operations, sustainment, and readiness including computing portfolio investment management.
Develop Continuity of Operations Planning	Establish a means to plan for the reconstitution of network operations to ensure continuous operations.
Develop Electromagnetic Frequency Assignments	This activity generates frequency assignments-an authorization for use of a specified range of the electromagnetic spectrum, at a specified location, with specified equipment, for a specified purpose, by a specified organization. Generation of frequency assignments takes into account capabilities of the spectrum-using equipment, prevention of harmful interference to other spectrum-using equipment, and any operational restrictions on frequencies available for use. "Permanent frequency assignments" are coordinated with host-nation spectrum management activities. Tactical frequency assignments address the day-to-day employment of the electromagnetic spectrum within the authorized permanent frequency assignments.
Develop Enterprise Services Capabilities	To design, develop, and test those enterprise services capabilities that support and enable net-centric operations.
Develop Enterprise Services Strategies, Policies, and Plans	This activity establishes current and future enterprise services goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for the transformation to a service-oriented environment. This activity provides guidance and direction that is used to determine what service capabilities are required to enable a service oriented and net-centric environment.
Develop Financial Services	Financial institutions are essentially information processors, and as such, all rely on telecommunications systems to maintain customer records, inform customers about services and accounts, and conduct financial transactions.
Develop GIG Capabilities	To design, develop and test capabilities required to share, take advantage of, and manage information in the GIG.
Develop GIG Infrastructure	This activity involves the design, development, and testing of the fundamental infrastructure required to support the Global Information Grid (GIG). Involves evolving the transport, computing, data, and assurance infrastructure.
Develop Global Information Grid (GIG) Capabilities	To evolve existing or build new infrastructure, information capabilities, and processes in support of a net-centric environment. It also includes the integration of technologies to support the infrastructure and information capabilities and the testing of the infrastructure, capabilities and processes.
Develop Information Capabilities	To design, develop and test capabilities required to share information in the GIG. Includes capabilities associated with posting and accessing information.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Develop Information Infrastructure Plan	Information Infrastructure plans are developed to support information sharing strategies and policies. Infrastructure plans should account for providing discovery, semantic and structural metadata to the GIG in enterprise federated registries, catalogs and/or directories. Information infrastructure should utilize defined COI ontologies and associate to enterprise-wide ontologies. Information infrastructure service levels should be provided to the GIG. Existing infrastructure should be utilized whenever possible to minimize the resource requirements for the deployment and maintenance of information infrastructure. Where a community is using existing data infrastructure, the information infrastructure plan should detail the plans for utilizing this infrastructure (e.g. service level agreements, etc.). This is a sub-activity under "Develop Net-Centric Data Strategies, Policies and Plans."
Develop Information Sharing Plan	An Information Sharing Plan is developed to implement the guidance defined in DoDD 8320.2 and associated information sharing policies (see "Define Information Sharing Policies"). This plan should detail the method of inventorying/prioritizing information assets, information asset publication procedures (in conformance to DoD-specified data publication methods and consistent with GIG enterprise and user technologies), metadata management requirements and other activities as needed to implement the goals of the Net-Centric Data Strategy. Recommended tagging guidelines to define rules and circumstances when tagging is appropriate, identify tagging levels (e.g., record-level, asset-level, inline) and methodologies for tagging information assets (e.g., automated, manual) should be developed. This plan should identify the information sharing capabilities required and will be utilized by the "Develop Data Infrastructure Plan" activity to determine the information infrastructure requirements.
Develop Integrated Implementation Plans	This activity considers the tenets of the strategies and policies and establishes an initial, high-level, integrated plan for implementing infrastructure, services, and other capabilities in support of a net-centric environment.
Develop Integrated Net-Centric IT Strategies, Policies, and Plans	To produce documents that establish the IT goals, objectives, processes, and plans for achieving a net-centric environment. Also addresses roles and responsibilities for all IT modernization, operations, sustainment, and readiness in support of a net-centric environment.
Develop Integrated NetOps Management Capabilities	This activity focuses on the functions of extending and evolving the Global Information Grid (GIG) infrastructure management, operations management, and protection capabilities. It includes defining, establishing, evolving, and integrating GIG NetOps functions in response to operational (mission) requirements. It includes the assignment of responsibilities and the identification of authorities for integrating management of newly extended or evolving GIG infrastructure. It is coordinated by NetOps personnel and implemented by NetOps administrators.
Develop Integrated NetOps Monitoring and Response Capabilities	This activity focuses on establishing integrated NetOps management and reporting responsibilities and capabilities for each new Global Information Grid (GIG) extension or evolution. It is performed by NetOps personnel and implemented by NetOps administrators. It takes policy, guidance, GIG NetOps management structures, and standard Net-centric operating procedures as controls. It produces new or revised integrated operational management and reporting capabilities for the NetOps personnel managing the GIG.
Develop Net-Centric Business Concepts	Provide conceptual guidance and direction for conducting business operations that take advantage of existing net-centric capabilities and influence future net-centric capabilities.
Develop Net-Centric Intelligence Concepts	Provide conceptual guidance and direction for conducting intelligence operations that take advantage of existing net-centric capabilities and influence future net-centric capabilities.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Develop Net-Centric Operational Concepts	Provide conceptual guidance and direction for conducting net-centric warfighter, business, and intelligence operations in DoD. These operations should take advantage of existing net-centric capabilities and influence the development of future net-centric capabilities.
Develop Net-Centric Processes	To construct processes that maximizes the use of and support capabilities in the GIG. These processes can be operational, managerial, or procedural in nature.
Develop Net-Centric Warfighter Concepts	Provide conceptual guidance and direction for conducting warfighter operations that take advantage of existing net-centric capabilities and influence future net-centric capabilities.
Develop NetOps Support Capabilities	This activity focuses on the functions of extending and evolving the Global Information Grid (GIG) infrastructure management, operations management, and protection capabilities. It includes defining, establishing, evolving, and integrating GIG NetOps functions in response to operational (mission) requirements. It pertains to the GIG Trust Infrastructure, protection mechanisms, sensor mechanisms, network management systems (e.g., Simple Network Management Protocol (SNMP)-based management), Network Facilities Management, Information Dissemination Management Systems (e.g., Global Broadcast System), and Net-Centric Core Enterprise Services Infrastructure.
Develop Network Capabilities	This activity focuses on the functions of extending and evolving the Global Information Grid (GIG) networking infrastructure. It includes defining, establishing, evolving, and integrating GIG networking functions in response to operational (mission) requirements. It pertains to network hardware, network media modes, network security, and network facilities.
Develop Network Management and Reporting Systems	This activity focuses on establishing the network management and reporting responsibilities and capabilities for each new Global Information Grid (GIG) extension or evolution. It is performed by NetOps personnel and implemented by NetOps administrators. It takes policy, guidance, GIG NetOps management structures, and standard Net-centric operating procedures as controls. It produces new or revised integrated operational management and reporting capabilities for the GIG.
Develop Network Services	The many functions that networks perform are known as services. Network services include: file services, print services, communication services, mail services, Internet services, and management services. In small organizations, one server may perform all these functions. In large organizations, several servers may be dedicated to any one of these functions.
Develop Satellite Services	The first uses of satellites were by the government in military, scientific research, public safety, and global communications applications. Satellites are best suited to services that must travel long distances or cover a wide geographical range
Develop Semantic and Structural Information Agreements	Communities of Interest support the Data Strategy goals of understandability and interoperability by developing semantic and structural agreements for data. In addition, these communities provide an organization and maintenance construct for facilitating the development of semantic (i.e., ontology) and structural (i.e., interoperability) information agreements. See "provide Community of Interest" for activities such as "Identify COI" or "Establish COI." Semantic and Structural metadata are provided to the NCE to facilitate visibility, accessibility, understandability and interoperability of information assets.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Develop Service	Service providers develop information services to enable net-centric sharing of information. Services should be implemented using open standards and loose coupling between data and applications. Services should adhere to applicable service description frameworks and provide access to information independent of business and presentation logic. Service providers should determine if GIG Enterprise Services (GES) or Core Enterprise Services (CES) are available to fulfill the capability needed prior to developing new services. Discovery of existing services and interfaces is described in activity "Discover Information Asset", "Access Information" and "Understand Information Asset". Services should be designed for scalability to the Enterprise to support the "unanticipated users" of Service Oriented Architectures.
Develop Software	This activity focuses on developing new software applications to fill a gap in required capability.
Develop Spectrum Management Strategies, Policies, and Plans	This activity establishes current and future spectrum management goals, objectives, and implementing plans and procedures, and assigns roles and responsibilities for all spectrum management modernization, operations, sustainment, and readiness in support of a net-centric environment.
Develop System and Network Logistics	This activity addresses coordinating logistics aspects (e.g., electrical power, contracted corrective- and preventative-maintenance, spare parts, storage media, air-conditioning, air-filtering, repair facilities, storage facilities, and facilities management including logistics in support of Force Protection Measures). This activity is performed by local-facility NetOps personnel and is coordinated through Command, Control, Communications and Computers (C4) Coordination Centers. It takes as inputs NetOps logistics needs and provides NetOps logistics provisioning plan(s). It is controlled by policy, guidance, standard NetOps operating procedures, and logistics management standards.
Develop System Protection Capabilities	This activity focuses on establishing the protection and anti-virus mechanisms computer hardware and associated software to be installed and integrated into the Global Information Grid (GIG) as part of a new and/or evolving functional capability. NetOps personnel perform this activity.
Develop Systems Management and Reporting Systems	This activity focuses on establishing the system management and reporting responsibilities and capabilities for each new Global Information Grid (GIG) extension or evolution. It is performed by NetOps personnel and implemented by NetOps administrators. It takes policy, guidance, GIG NetOps management structures, and standard Net-Centric operating procedures as controls. It produces new or revised integrated operational management and reporting capabilities for the GIG.
Develop Technologies	This activity comprises the necessary steps for determining availability of a technology, developing or acquiring the required technology, if it is not available.
Develop Wireless Transmission Services	Wireless transmission offers many advantages over wire-bound transmission. When engineers talk about wireless transmission, they refer to the atmosphere as an unguided medium. Because the air provides no fixed path for signals to follow, signals travel without guidance i.e. cellular communications.
Develop/Update Information Sharing Architectures	New and/or existing information sharing architectures are created and/or updated to support planned information sharing capabilities. The architecture should depict components that emphasize the discovery, services-based approach to systems engineering, metadata use to support mediated information exchange and web-based access to information assets. Information Sharing Architectures should align with the NCOW-RM and other appropriate Enterprise architectures. This is a sub-activity under "Develop Net-Centric Information Strategies, Policies and Plans."

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Educate Net-Centric Information Sharing Practices	Promotional and educational campaigns are developed to facilitate the adoption of Net-Centric Data Strategy Goals. Best practices show that new operating practices are assimilated more quickly when coupled with promotional and educational activities. Lessons learned while evolving the GIG should be consolidated and provided to the GIG to facilitate future learning. This is a sub-activity under the "Institutionalize Data Activities."
Engineer Network Protection Capabilities	This activity focuses on establishing the protection and security functions for the network hardware, network media modes, and network facilities of the Global Information Grid (GIG) networking infrastructure.
Engineer System Software	This activity focuses on selecting, sizing, and loading the system software that operates the Global Information Grid (GIG) infrastructure or is used to administer the GIG infrastructure (e.g., Operating Systems, System Utilities, Data Management Systems, Auditing Software, and System Management and Reporting Applications, Monitoring Software). It takes hardware configurations, GIG architecture information, and Standard Net-Centric Operating Procedures, and supplies system applications that run and manage the GIG. The planning and engineering are constrained by hardware configurations, standard NetOps (Net-Centric) operating procedures, and the quantity of administrative domains being supported.
Engineer Transmission and Switching Systems	This activity focuses on providing new Local and Wide Area information transport capabilities through the engineering of new bandwidth, physical wiring, router topologies, and switching capabilities, wireless transmission cells, gateways and Public Switched Telephone Network (PSTN) isolation, etc. It takes desired information transport capabilities as input. It is controlled by policy, guidance, networking "best practices," existing resources (including commercial provisioning capabilities), connectivity requirements, environmental constraints, and optimizing of information flows. It produces new or evolved integrated extensions to the Global Information Grid (GIG) information transport capabilities.
Establish Administrative Boundaries	To determine and set the scope for areas of administration within the GIG to facilitate control and establishing responsibility.
Establish NetOps Functions	Incorporate required set of functions associated with network operations.
Establish Network Boundaries	Determine and fix the specific scope and extent for the various networks within the GIG.
Establish Reporting Hierarchy	Develop a hierarchical structure that describes the required path for reporting about network operations.
Establish Service Provider	<p>The choice of a service provider depends on the amount of bandwidth you need and the SLA offered by the provider. Large global providers offer a minimum OC-12 (622 Mbps)</p> <p>backbone in a fully meshed architecture. In a meshed architecture there are multiple alternate pathways so that if one part of the network is disabled, the carrier is automatically rerouted to another path without the customer's knowledge. Smaller providers offer</p> <p>slow-speed connections that vary from 64 Kbps to 622 Mbps and typically limit the number of router hops to two.</p>
Establish Theater Injection Point	Set-up and implement a physical communications node within Theater to provide required tactical reach-back capability.
Evaluate Technologies	To assess the effectiveness and suitability of the technology with respect to the capability it supports.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Evolve Assurance Infrastructure	This activity involves the design, development, and testing of the assurance infrastructure increments required to support the net centric environment. Includes NetOps and Information Assurance, and leverages the current assurance infrastructure.
Evolve Communications Infrastructure	Telecommunications services are three categories: voice, video, and data. Voice telecommunication refers to any means of using electrical signals to transmit human voice across a distance, such as telephones and radio broadcasts. Video telecommunication refers to the electrically-based transmission of moving pictures and sound across a distance, such as TV broadcasting or distributing live feeds of an event to the screens of networked computers. Data telecommunication refers to the use of electrical signals to exchange encoded information between computerized devices across a distance.
Evolve Computing Infrastructure	This activity focuses on the functions of extending and evolving the Global Information Grid (GIG) computational infrastructure. It includes defining, establishing, evolving, and integrating GIG computing functions in response to operational (mission) requirements. It pertains to computing hardware, software, and data operations. Leverages existing computing infrastructure.
Evolve IA Infrastructure	This activity involves the design, development, and testing of the Information Assurance (IA) infrastructure increments required to support the net centric environment. Leverages existing IA infrastructure.
Evolve Information Infrastructure	This activity involves the design, development, and testing of the data infrastructure increments required to support the net centric environment. Includes the development of metadata products that support information exchange (e.g. they are the foundation for instance documents and drive run-time interoperability).
Evolve NetOps Infrastructure	This activity involves the design, development, and testing of the NetOps infrastructure increments required to support the net centric environment. Leverages existing NetOps infrastructure.
Evolve the Global Information Grid (GIG)	Actions to orchestrate the continuous, controlled, and synchronized transformation of the existing information environment to a net-centric environment (GIG). Focuses on what decision-makers and developers must think about to guide, architect, develop, and implement an effective GIG that supports and enables the conduct of net-centric DoD operations. Involves the evolution of the enterprise information infrastructure, capabilities, and processes to a GIG.
Evolve Transport Infrastructure	To design, develop, and test the transport infrastructure increments required to support the net centric environment. Leverages the current transport infrastructure.
Govern GIG IT Portfolio Investment	This activity assesses the performance of the current IT portfolio investments against current and future needs and directs changes in funding and/or portfolio contents necessary to ensure the IT portfolio investments are meeting established performance requirements.
Govern Global Information Grid (GIG) Evolution	To control, direct, and influence the way the net-centric environment evolves. Pertains to the policy, management, and general oversight regarding the development of the net-centric environment. Includes activities to govern IT portfolio investment, control capability increment integration, and institutionalize key net-centric strategies.
Govern Information Sharing Activities	Information sharing activities are governed with sustained leadership commitment to support compliance to developed "Net-Centric Information Sharing Plans." Information sharing metrics are analyzed and appropriate actions are taken to ensure activities are conducted according to plan. This is a sub-activity under "Institutionalize Net-Centric Information Sharing Capabilities."

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Govern Legacy IT Portfolio Investment	This activity assesses the performance of the legacy components in the current IT portfolio investments (i.e. sustainment and readiness) against current and future needs and directs changes in funding and/or legacy portfolio component contents necessary to ensure the overall IT portfolio investments are meeting established performance requirements.
Govern Modernization IT Portfolio Investment	This activity assesses the performance of the modernization components in the current IT portfolio investments against current and future needs and directs changes in funding and/or modernization portfolio component contents necessary to ensure the overall IT portfolio investments are meeting established performance requirements.
Guide and Direct Global Information Grid (GIG) Evolution	To influence the transformation of DoD's existing information environment to a net-centric environment (GIG) with general and specific guidance and direction that promotes a common azimuth for achieving an GIG. The guidance and direction may include a vision, descriptions of specific elements, or a specified approach. This activity includes the development of strategies, policies, plans, and concepts that establish goals, objectives, and implementation guidance for evolving the GIG.
Identify Authorities for Managing Integration of Functions	Establish authoritative entities for managing the integration of functions.
Identify Authorities for Overseeing and Controlling NetOps Reporting	Determine and select authoritative entities to oversee and control the reporting of network operations.
Identify Authorities for Oversight and Control of Networks	Select and authorize entities to provide oversight and control of the networks within the GIG.
Identify Authorities to Oversee and Control Actions	Determine the responsible entity for supervising and controlling actions within specified boundaries of the GIG.
Identify GIG Desired Situational Awareness Capability	Determine the level of functionality required for a situation awareness capability associated with network operations.
Identify Information Assets	Information asset owners (e.g. system owners, information producers, information management staff, COIs) determine what information assets (documents, images, metadata, services, etc) are produced or controlled within their community, which information assets have the highest priority for visibility/accessibility, and who are the authoritative sources. This set of activities support Users in determining the full set of assets available across the Community and determining the priority for accessibility. However, all information assets should be visible to the GIG, even if they are not accessible.
Identify Key Interfaces	Key interfaces (human or machine) for facilitating information sharing are identified. COIs should consult the Net-Centric Key Interfaces Profile (KIPs) to leverage and conform to specifications defined in the KIPs. The interface specification standards helps to ensure the compatibility of developed interfaces that will enable the "many-to-many" exchanges of a net-centric environment. A Net-Centric KIP is a net-centric boundary where systems must be interoperable at that interface to transit and access enterprise services in the GIG. These interface spans organizational, multi-net network and enterprise service boundaries, and they are configuration managed at the program management level with DOD level oversight. KIPs is maintained in the DoD IT Standards Repository (DISR), and managed by IT Standards Committee. This is a sub-activity under "Develop Semantic and Structural Information Agreements."
Identify NetOps Logistics Needs	Determine what resources are required for support network operations.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Implement Global Information Grid (GIG) Capabilities	To activate and place developed capabilities into the net-centric environment. Includes the integration and activation of developed infrastructure, information capabilities, and processes. Capability increments must include both physical and technical security as previously planned and developed.
Implement Net-Centric Processes	To activate and integrate developed processes that maximize the use of and support capabilities in the GIG. These processes can be operational, managerial, or procedural in nature.
Institutionalize Enterprise Services	The activity supports the institutionalization of the Enterprise Services Strategy through sustained leadership commitment to approved strategies, policies and plans. Organizations should promote and sustain the principles of the Enterprise Services Strategy as they apply.
Institutionalize Information Assurance	The activity supports the institutionalization of the Information Assurance Strategy through sustained leadership commitment to approved strategies, policies and plans. Organizations should promote and sustain the principles of the Information Assurance Strategy as they apply.
Institutionalize Net-Centric Information Sharing Capabilities	Information sharing approaches are incorporated in processes and practices through sustained leadership, education and promotion. Communities of Interest have active participation of members; including participation in DoD-wide governance efforts. Information quality is increased through responsiveness to user needs.
Institutionalize Net-Centric Strategies	The activity supports the institutionalization of the key Net-Centric Strategies through sustained leadership commitment to developed strategies, policies and plans. All DoD organizations should promote and sustain the principles of each strategy, policy, and plan as they apply.
Integrate Supporting Technologies	This activity involves the migration of technologies to standards, and the integration of standards into infrastructure and services capabilities. It aggregates the functions of developing and evaluating technologies for selection as standards, and applying the set of standards that are essential to the effective and efficient implementation of the information environment. This activity may be initiated as a result of emerging technology, activities of commercial standards bodies or consortia, or a recognized need to reduce the variety of standards being used within the information environment.
Inventory Information Assets	Information asset owners (e.g., system owners, information producers, and information management staff) inventory their information assets to compile a complete list of assets with the community. This listing will be used by the COI to prioritize information assets for accessibility to the GIG. All information assets should be visible to the GIG, even if they are not accessible. A full information asset inventory will also support the Community in determining the authoritative sources and identifying duplicative information assets. Information assets are aligned to appropriate IT portfolios. This information asset inventory should be updated and maintained on a regular basis to ensure that the COI has visibility into the assets of the community. This is a sub-activity of "Identify Information Assets."
Load Software	To place software on a physical device or add software to existing software for execution.
Monitor Emerging Industry Policies	Since the Telecommunications Act of 1996, policies governing the telecommunications industry in the United States have continued to evolve. Meanwhile, new and old telecommunications (voice, video, and data) providers, as well as lobbying organizations that promote citizen interests, continually challenge the latest policies. Because the network is public, its services are regulated by the FCC and the state public utilities commissions.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Nominate Frequencies	<p>This activity is performed to initially identify desired frequencies that are interference free.</p> <p>Source: Department of Commerce, Office of Radio Frequency Management</p>
Perform Interference Analysis	<p>This activity is performed to predict potential interference conflicts of near frequency assignment proposals, identify potential sources to existing frequency assignments, and nominating new frequencies.</p> <p>Source: Department of Commerce, Office of Radio Frequency Management</p>
Perform National Telecommunications and Information Administration Review	<p>This activity is required for all frequency assignments every five years, by the National Telecommunications and Information Administration, to evaluate future allocations of those assignments. Additionally, organization validates the accuracy of the nominated frequency assignments to evaluate the effects of spectrum congestion, competing systems, and interoperability on various operational limitations such as geographical restrictions, transmitted power, antenna height and gain, bandwidth, etc.</p> <p>Source: Department of Commerce, Office of Radio Frequency Management</p>
Perform Technology Forecast	<p>This activity focuses on the future CI products and the availability of associated software and maintenance infrastructure with the objective of installing and integrating future computational capabilities into the Global Information Grid (GIG) as part of a new and/or evolving functional capability supporting operational needs.</p>
Plan Information Sharing Capabilities	<p>Information sharing capabilities are planned through the development of associated policies, strategies and plans. Policies are developed to extend the guidance in DoDD 8320.2, information sharing plans are developed to define how information will be shared and infrastructure sharing plans are developed to determine the system requirements. These plans are reflected in associated architectures and metrics developed to support governance.</p>
Prioritize Information Assets	<p>Information asset owners (e.g., system owners, information producers, information management staff), through participation with their COI, prioritize information assets for accessibility in the GIG. Prioritization of information assets can be accomplished using a variety of criteria (e.g. highest value to expected users, usage frequency, etc.) as determined at the discretion of the community. Highest priority information assets should be made accessible and understandable to the GIG. Information asset priorities should reflect provided user feedback (see "Respond to User Feedback"). All information assets should be visible to the GIG, even if they are not accessible. This methodology should be maintained as part of regular planning processes. This is a sub-activity under the "Identify Data Activities."</p>
Produce Standard NetOps Status Reporting Procedures	<p>Develop standard reporting procedures to convey the status of network operations.</p>
Promote Information Sharing	<p>Information practices and procedures are promoted to support institutionalization of the Net-Centric Data Strategy. Incentives should be developed and provided to the pertinent Communities to encourage participation in the net-centric data activities. This is a sub-activity under the "Institutionalize Net-Centric Information Sharing Activities."</p>
Protect Data and Networks	<p>The ability to deliver Defense-in-Depth protection of the GIG.</p> <p>Amplification: This capability puts in place and actively manages the preventative measures required to minimize the GIG's vulnerability to attacks and unexpected events.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Provide Access to Shared Computing Infrastructure Resources	<p>The ability for authenticated users and trusted machines to access shared CI resources regardless of location or access device.</p> <p>Amplification: The ability to provide appropriate CI interfaces and access mechanisms that enable secure robust, agile, virtual provisioning and allocation of shared data storage and processing resources to the edge</p>
Provide Adaptable Hosting Environments	The ability to provide fixed global/regional enterprise facilities and adaptable virtual hosting environments to the edge for sharing applications, operating systems, and services.
Provide Assurance Infrastructure	To activate and integrate developed assurance infrastructure increments into the net-centric environment. Assurance infrastructure increments include NetOps and IA elements.
Provide Assurance Services	To activate and integrate developed assurance capabilities into the net-centric environment. Assurance capabilities involve NetOps and IA elements and support assured networks and assured information sharing.
Provide Authorization and Non-Repudiation	<p>The ability to identify and confirm a user's authorization to access something on the GIG and clearly show who took what actions on the GIG.</p> <p>Amplification: This capability provides a critical security service that underpins many of the other GIG capabilities.</p>
Provide Automated Status Reporting	All GIG CI resources will continually report their status, thus enabling NetOps to have a continuous view of the status of computing resources across the GIG for situational aware and command and control purposes.
Provide Certification and License Training Resources	<p>This activity is performed to ensure that adequate technical training resources are available for conducting various procedures that require highly-trained personnel to run them.</p> <p>Source: Steve Sudkamp (NNWC)</p>
Provide Commodity Computing	Providing interoperable computing environment that can host multiple application or services
Provide Computing Infrastructure	To activate and integrate developed computing infrastructure increments into the net-centric environment. Computing infrastructure increments must include both physical and technical security as previously planned and developed.
Provide Deployable, Scalable GIG Capabilities	<p>Common Infrastructure Environment</p> <p>The ability to provide computing infrastructure and communications to GIG "Edge" and trusted "Unanticipated"" users on-demand (e.g., content staging, forward staging, caching).</p> <p>Amplification: The ability to quickly provide highly available, accessible, dynamic, modular enterprise resources, net-centric CI processing, storage, and retrieval; and scalable storage and processing capacity on demand to warfighters, 'edge' users, trusted "unanticipated" users, and support personnel. The desired effect is to support net-centric interoperability, distributed applications, data sharing, and collaboration.</p>
Provide Distributed Computing Infrastructure Functionality	<p>The ability to provide distributed computing, data storage, and shared spaces across the GIG for data and information sharing.</p> <p>Amplification: The ability to provide robust and agile computing infrastructure that enables trusted users to access and share data and information efficiently and effectively anywhere they are located, across functional, security, national and interagency domains.</p>

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Provide Dynamic, Automated Storage Provisioning	Data storage will be automatically allocated heuristically, based on usage patterns and real-time capacity requests. Thus, CI, will be able to "learn" from past usage experience to better serve users.
Provide Enterprise Services	To activate and integrate developed service capabilities into the net-centric environment.
Provide IA Training and Awareness	Develop and provide materials, classes, instruction and policy regarding training for and awareness of IA capabilities for the GIG.
Provide Information Transport	<p>Information Transport is the ability to transport information, data and services anywhere on the GIG.</p> <p>Amplification: This capability ensures that the right infrastructure is in place to provide transport between and among end-user devices and the processing and storage of the GIG. It also puts in place the ability to expand the infrastructure dynamically based on operational needs (on-demand capacity).</p>
Provide Internet Services	<p>Include World Wide Web servers and browsers (for example, Internet Explorer or Netscape), file transfer capabilities, and a means for directly logging on to other computers on the Internet. After you establish a connection, your workstation and the servers it relies upon must run standard protocols to use the Internet's features.</p>
Provide Location-Independent Storage	
Provide Machine to Human Interfaces	The service providers provide interfaces for the human users to access the information services available in the GIG. The human interface may be a graphic user interface (GUI) that can display the requested data on the user's information access device (e.g., laptop, desktop, PDA, cell phone). Service providers may provide machine-to-machine interfaces in addition to machine-to-human. Services should adhere to published interface specifications (e.g., discovery interface specification). This is a sub-activity under "Provide Service Interfaces."
Provide Machine to Machine Interfaces	Service providers provide interfaces for machines to access information services available in the GIG. The machine interface may be a web service that allows machines to exchange secure messages. Service providers may provide machine-to-machine interfaces in addition to machine-to-human. Services should adhere to published interface specifications (e.g., discovery interface specification). This is a sub-activity under "Provide Service Interfaces."
Provide Net-Centric Information Services	To activate and integrate developed information capabilities into the net-centric environment. Information capabilities consist of services and resources that support assured information sharing and assured collaboration.
Provide Net-Centric Infrastructure	To activate and integrate developed infrastructure increments into the GIG. Infrastructure increments include both physical and technical security as previously planned and developed.
Provide NetOps Logistics Provisioning Plan	Develop and make available a plan for the provisioning of network operations logistics.
Provide Semantic Metadata to NCE	Semantic metadata, such as COI developed ontologies (data categorizing schemes, thesauruses, vocabularies, key word lists, and taxonomies) are registered in an enterprise federated metadata registry (e.g. DoD Metadata Registry). Semantic metadata should be accessible from discovered information assets to facilitate understanding (e.g., an associated vocabulary for an information asset should be accessible without requiring an additional discovery process). Registered semantic metadata should provide associations to Enterprise-wide semantic metadata to ensure understandability of information assets across the Enterprise. This is a sub-activity under "Develop Semantic and Structural Information Agreements."

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Provide Service	Service providers develop and provide discoverable services to the GIG. Service levels are defined and provided to the GIG. Interfaces are developed to support both human and machine users. Service metadata (discovery and performance) is provided to the GIG to facilitate the goals of the Net-Centric Data Strategy.
Provide Service Interfaces	Service interfaces are provided to support both human and machine users. These interfaces should be non-proprietary, accessible through web-based methods and adhere to applicable GIG policies and specifications. Service interfaces should reflect provided user feedback (see "Respond to User Feedback"). Provided interfaces should conform to defined GIG Key Interface Profiles (KIPs) which provide a description of required operational functionality, systems functionality, and technical specification for the interface (DoDD 5101.7). This is a sub-activity under "Provide Service."
Provide Service Metadata to GIG	DDMS compliant service discovery and structural metadata is provided to enterprise federated service registries. A enterprise federated service registry is any mechanism which can be searched to determine the existence of services and applicable service interfaces (e.g., UDDI). Service directories should utilize available Community or Enterprise developed ontologies to support the understanding of information assets across the Enterprise. This is a sub-activity under "Provide Service."
Provide Service Performance, Operational State and Availability to GIG	Performance, operational state and availability data for services should be visible to the Enterprise. This information should support provided service levels and be available for service users. This is a sub-activity under "Provide Service."
Provide Service to GIG	Service providers provide users access to services. Access shall be limited based on applicable law, policy, and/or security classification. Service providers should establish the process and procedure to manage changes to the service and communicate anticipated changes to the user communities in the GIG. Any changes to services (e.g., location, structure, interfaces) should be scheduled and reflected in updates to service metadata registered in enterprise federated service registries. Services should utilize available Information Assurance (IA) Core Enterprise Services (CES) for access control. This is a sub-activity under "Provide Service."
Provide Structural Metadata to GIG	Structural metadata (e.g. format-related metadata, schemas, COI extension to DDMS, web service tags, access control metadata, etc) used to facilitate interoperability should be registered in a enterprise federated metadata registry (e.g., DoD Metadata Registry) so users may discover and understand more about how the data might be used. Registering metadata components to the DoD Metadata Registry supports many-to-many interoperability by providing system architects and developers with insight into existing data schemas that they can employ and extend. Discoverable services should provide an association to registered structural metadata to facilitate interoperability. This is a sub-activity under "Develop Semantic and Structural Information Agreements."
Provide Transport Infrastructure	To activate and integrate developed transport infrastructure increments into the net-centric environment. Transport infrastructure increments must include both physical and technical security as previously planned and developed.
Respond to User Feedback	User perspectives are incorporated into information sharing approaches through continual feedback. Ratings processes are established to evaluate and refine the user experience. The feedback and ratings process, coupled with improved information asset visibility, will increase the integrity and quality of data. Feedback process additionally supports the identification of previously unanticipated users. This is a sub-activity under the "Institutionalize Net-Centric Information Sharing Activities."
Retire Standards	This activity is responsible for discharging obsolete and outdated standards that are no longer required.

NCOW RM v1.2 Activity Definitions

Activity Name	Activity Definitions
Scale Software	Determine the level of software functionality required to meet needs and size software to meet the parameters of the physical device where it will reside.
Secure Information Exchanges	<p>The ability to secure information exchanges that occur on the GIG with a level of protection that is matched to the sensitivity of the exchange and the risk of compromise.</p> <p>Amplification: This capability establishes the standards and tools to secure information exchanges, as well and puts in place and monitors the processes and controls necessary to ensure security.</p>
Select Software	Identifying and choosing the appropriate software to fulfill a need.
Select Standards	This activity comprises the necessary steps to determine which technologies should become DoD standards.
Support Grid Computing	Net-centric CI will leverage the distributed computing resources of the GIG over local and wide area networks to provide computing service that appears to the end user or application as one large, virtual computing capability.
Test Computing Infrastructure	Involves developmental and operational testing of the individual components and completely integrated computing infrastructure.
Test NetOps Support Capabilities	This activity involves the developmental and operational testing of NetOps support capabilities prior to implementation.
Test Network Capabilities	This activity involves the developmental and operational testing of all network capabilities prior to implementation.
Virtualize Application Environments	Applications will be hosted in shared versus dedicated environments, enabling dynamic changes to processor and storage capabilities depending upon usage patterns. Hosting environments provide seamless access to all applications and services regardless of their physical location.