

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
<b>Connect, Access and Share</b>	<b>The set of capabilities enabling interoperability across mission areas and organizations internal and external to DoD and giving users the ability to find, access, provide, share, process, and manage information and other services .</b>			
<b>Connect</b>	<b>The set of computing and communications infrastructure capabilities enabling any user or service to reach any other user or identify and use any other service.</b>			
Infrastructure Provisioning	The ability to provision and allocate shared computing and data storage resources in a computing platform agnostic, location independent, transparent, and real-time manner.	A3.1.1.1 Provide Services Infrastructure A3.2.1.2.1.3 Enable Dynamic, Virtual Processing in Computing Infrastructure A4.2.3.1 Allocate IE Resources	CIR 01 CIR 05 CIR 06	S1.1.6.1 Storage On Demand Services S1.1.6.2 Computing On Demand Services S1.3.6.1 Software as a Service S1.3.6.2 Infrastructure as a Service S.1.3.6.3 Platform as a Service
Interoperable Components	The ability of the components of the IE to interoperate with one another and with mission partners to support mission needs and in accordance with Law, Regulation, and Policy (LRP).	A3.2.1.2.6 Provide Grid Computing Environment A3.2.2.1 Procure Interoperable Transport Components A3.2.2.2 Standardize Extensions to Other Network Infrastructures	GP 02 DSDR 06 CIR 02	
Assured End to End Communications	The ability to deliver the information transport required for assured end-to-end communications. This capability enables a joint infrastructure providing global, interoperable communications across the DoD IE and with mission partners.	A3.2.2.1 Procure Interoperable Transport Components A3.2.2.2 Standardize Extensions to Other Network Infrastructures A3.2.2.3 Provide Global Connectivity A3.2.2.4 Provide Communication Support Mechanisms A4.2.3.1.1.1 Plan Communications Resource Allocation A4.2.3.1.1.6 Manage Satellite Communications (SATCOM)	CRR 01 CRR 02 CRR 04 CRR 05	S1.1.7 End User Device Services S1.1.1 Commercial Satellite Communications Services S1.1.2 IP Based Networking Services S1.1.3 Video Teleconferencing Services S1.1.4 Wireless Communications Services S1.1.5 Wired Communications Services

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
Unified Communications and Collaboration	The ability to seamlessly integrate voice, video, and data applications services so they are delivered ubiquitously across a secure and highly available single protocol network infrastructure.		CRP 01 CRR 01	S1.1.2.1 Video over IP Services S1.1.2.2 Voice over IP Services S1.1.2.3 VPN Services
Global Connections	The ability to connect users anywhere in the DoD IE to required applications, services, and systems so they are able to effectively use these resources. This capability provides connectivity to all nodes and users, including: those changing their points of attachment among operational and network domains and/or COIs; key fighting, reconnaissance, and administrative systems regardless of platform; legacy systems remaining in the force; and mission partners. Connectivity anywhere on the globe is guaranteed even in austere environments. Network connectivity is provided to end points (such as WAN / LAN and direct connections to mobile end users) in the same or different autonomous systems.	A3.1.3.2.2 Provide Common End User Interfaces A3.2.2.2 Standardize Extensions to Other Network Infrastructures A3.2.2.3 Provide Global Connectivity A4.2.3.1.1.6 Manage Satellite Communications (SATCOM)	GP 06 SIP 02 CRR 02	S1.1.7 End User Device Services S1.1.1 Commercial Satellite Communications Services S1.1.2 IP Based Networking Services S1.1.4 Wireless Communications Services S1.1.5 Wired Communications Services
Operational Bandwidth Assessment	The ability to determine and analyze the operational bandwidth implications of applications and services prior to fielding and account for those implications during implementation.		CIR 03	
Internet Connectivity	The ability to enable a globally open, stable, and secure Internet to allow collaboration and cooperation within the Department and with mission partners. This capability requires the development of international cyberspace legal frameworks, working internally within DoD and externally with international partners, to increase the security and stability of the Internet. It also requires the advocacy of DoD equities at international technical and governance meetings for the Internet.	A2.3.4.2.2 Protect Data-in-Transit Between NIPRNet and Internet A3.2.2.2 Standardize Extensions to Other Network Infrastructures		S1.1.2 IP Based Networking Services
Spectrum Management	The ability to manage the electromagnetic spectrum to enable flexible, dynamic, non-interfering spectrum use. Provides assured access to and management of the electromagnetic spectrum. Spectrum management policies are established and automated tools are available to promote a collaborative environment and are made accessible to authorized users. Integrates spectrum management capabilities and tools into the planning and execution of operations and provides the capability to monitor spectrum use.	A1.1.2.6 Develop Joint Spectrum Assignment Plan A4.2.3.1.1.5 Allocate Electromagnetic Spectrum	CRR 06	

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
Ad Hoc Networks	The ability to deploy and install ad hoc networks in support of mission needs. Sensor-to-shooter networks will be constructed at will to engage all types of targets as they develop. Resulting networks will be fully connected, able to dynamically adapt to new situations and transition from "cold" to "hot" operational missions. Automated tools will be provided to network managers to allow them to deploy networks with minimal manual intervention, based on operational guidelines and Commander's guidance, by geographical area.	A3.2.1.1 Implement Joint Computing Infrastructure A3.2.2.3.2 Provide Local Area Network (LAN) Connectivity A3.2.2.3.3 Provide Ad Hoc Connectivity A4.2.3.1.1.3 Support Multiple Military Operations	CRR 02	S1.1.2.4 Ad Hoc Network Services
<b>Access</b>	<b>The set of capabilities enabling the granting or denying of available information assets to both human and machine users.</b>			
Identity Provision and Management	The ability to provide and manage assured digital identities for all users, services, and devices.	A1.1.2.9.2 Develop Identity Management and Authentication (IdM&A) Policy A2.1.1 Provide Identity Management and Authentication A2.1.3 Provide Federation	SAR 07 OPR 01 OPR 04	S1.2.2.2 Identity Management Services S1.2.2.3 Authentication Management Services S1.3.8 Audit Services
Credential Provision and Management	The ability to provide and manage common and portable identity credentials for users, services, and devices to provide visibility of, and access to, all services and applications.	A1.1.2.9.2 Develop Identity Management and Authentication (IdM&A) Policy A2.1.1.2 Provide Credentialing Mechanisms	SAR 07 OPR 01 OPR 04	S1.2.2.4 Credential Management Services
Access Control	The ability to ensure only authenticated and authorized users are able to access and use DoD IE resources, in accordance with established policies.	A1.1.2.9.2 Develop Identity Management and Authentication (IdM&A) Policy A1.1.2.9.3 Develop Access Control Policy A2.1.1.1.3 Expose Identity Information A2.1.3 Provide Federation A2.1.2 Provide Access Control A2.1.4 Monitor Authentication and Access Control A2.1.5 Manage Digital Rules	SAR 07 SAR 08 OPR 02 OPR 05 OPR 06	S1.2.1 Access Control Services S1.2.2.1 Authentication Management Services S1.3.8 Audit Services

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
Digital User and Service Attributes	The ability to provide digital user and service attributes to enable functionality such as access control and enterprise e-mail.	A2.1.1.1.1 Register Identity A2.1.1.1.2 Maintain Identity A2.1.1.1.3 Expose Identity Information A2.1.2.1.1 Identify Standard Attributes A2.1.3.2 Synchronize and Deconflict DoD IA Attributes A3.1.1.3.2.1.2 Maintain Entity Attributes A3.1.1.3.2.2.2 Expose Entity Attributes	SAR 07	S3.2.1 Digital Access Policy Management Services S1.2.2.3 Attribute Management Services
<b>Share</b>	<b>The set of capabilities enabling information and information assets to be used within and across mission areas.</b>			
Data and Functionality as Services	The ability of all authoritative data and associated capabilities to be provided as services in the IE.	A3.1.1 Provide Enterprise Services A3.1.2 Provide End User Services and Applications A3.1.3 Enable User Trust and Utility of IE	All DSD Rules	S1.3.1.1 Content Discovery Services S1.3.1.2 Content Delivery Services S1.3.2.1 Information Sharing Services S1.3.2.2 Cross Domain Services S1.3.3.1 Enterprise E-mail Services S1.3.3.2 Social Networking Services S1.3.3.3 Instant Messaging Services S1.3.4 Standard Web Office Applications Services S1.3.5 Custom Application Services S1.3.6.1 Software as a Services S1.3.6.2 Infrastructure as a Service S1.3.6.3 Platform as a Service S1.3.7 Language Translation Services S1.3.8 Audit Services S1.1.7 End User Device Services

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
Collaboration	The ability to collaborate in real-time, both internally and with external mission partners. Collaboration is one means to accomplish information and knowledge sharing.	A2.2 Enable Cross Domain Security A3.1.1.4.1 Provide Other Collaboration Services A3.1.1.4.3 Provide Awareness Services A3.2.1.2.9.2 Enable Secure Interoperability A5.2.2 Collaborate A3.2.2.2 Standardize Extensions to Other Network Infrastructures	GP 05 OPR 11	S1.3.3.1 Enterprise Email Services S1.3.3.2 Social Networking Services S1.3.3.3 Instant Messaging Services S1.3.2.2 Cross Domain Services
Data and Service Availability	The ability to discover and use trusted data, services, and information across the enterprise.	A2.1.2.2.1 Manage Trust Negotiation A3.1.1.3.3 Provide Discovery Services A3.1.3.1.1 Manage Availability A3.1.3.1.3 Manage Authenticity A3.2.1.2.9.3 Provide Trusted Computing A5.1 Locate and Use Information, Services and Applications A2.7 Tag Data Objects with IA Metadata	DSDR 02 DSDR 03 DSDR 06 DSDR 04 DSDR 07 DSDR 12 SIR 01 CIR 06 OPR 10	S2.2.1 Security Metadata Management S1.3.1.1 Content Discovery Services S1.3.1.2 Content Delivery Services
Knowledge Sharing	The ability to share knowledge across the IE and with external partners. Knowledge sharing can be accomplished via collaboration as well as with other means.	A1.1.2.7 Develop Information Sharing Policy A2.2 Enable Cross Domain Security A3.2.1.2.3 Provide Storage Environment A3.2.1.2.7.2 Provide Computing Infrastructure Storage Services A3.2.1.2.9.1 Enable IA for Shared Storage and Media Functions A5.2 Share Information	DSDP04 CIRP 01 CIR 02 CIR 05 OPR 09 OPR 11 OPR 15	S1.3.2.1 Information Sharing Services S1.3.2.2 Cross Domain Services S1.1.6.1 Storage On Demand Services S1.1.6.2 Computing On Demand Services

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
Information Sharing with Mission Partners	The ability to share information with multi-national and other mission partners.	A1.1.2.7 Develop Information Sharing Policy A2.2 Enable Cross Domain Security A3.2.2.2 Standardize Extensions to Other Network Infrastructures A4.2.3.1.1.5.2 Enable RF Communications with Mission Partners A5.2 Share Information	GP 05 DSDP 04 CIRP 01 CIR 02 CIR 05 OPR 09 OPR 11 OPR 15	S1.3.2.1 Information Sharing Services S1.3.2.2 Cross Domain Services
Foreign Language Processing	The ability to process and use information presented in a foreign language.			S1.3.7 Language Translation Services
Multi-Source Data Fusion	The ability to integrate and fuse multi-source data and information into usable products, intelligence, and decision-making information.			
Information Dissemination Management	The ability to develop and enforce information dissemination priorities. This capability manages DoD IE resources to provide information dissemination based on dynamically set information priorities. It provides the user with timely information reporting on the status of information delivery against stated requirements. With this capability, Commanders at all levels and COIs will be able to define their needs and requirements for information and information dissemination and will know when information requirements cannot be met.	A4.2.5 Perform Content Management	CIR 03 NOAR 02	S1.3.2 Information Management Services
<b>Operate and Defend</b>	<b>The set of capabilities for managing the operation of the IE to ensure networks, services, and underlying physical assets can be dynamically allocated and configured, and data and services are secured and trusted across DoD.</b>			
<b>Operate</b>	<b>The set of capabilities providing real-time situational awareness, protection, and operational management of the IE.</b>			

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
Continuity of Operations	The ability of the infrastructure to be survivable, resilient, redundant, and reliable in the presence of attack, failure, accident and natural or man-made disaster. This capability ensures segments of the network have the ability to “fail” without causing failure to other parts of the IE so the operational mission continues.	A3.2.2.4.1.2 Facilitate Continuity of Communications Service A4.2.3.3 Provide Change Management A3.2.1.4 Maintain Computing Infrastructure	SIP 01 SIR 02	S1.1.6.1 Storage On Demand Services S1.1.6.2 Computing On Demand Services S1.3.6.1 Software as a Service S1.3.6.2 Infrastructure as a Service S1.3.6.3 Platform as a Service S2.1.1 Change Management Services
IE Health and Readiness Measurement	The ability to develop and maintain metrics required to measure the health and mission readiness of DoD IE assets, services, and applications.	A1.1.2.3 Develop Quality of Service (QoS) Policy A4.1.3 Monitor Accomplishment of Commander's Intent for NetOps A4.2.3.7.1 Develop and Apply IE Performance Metrics	NOAR 07	
IE Situational Awareness	The ability to collect, analyze, and share situational awareness data and information for effective IE operation and defense. Provides the ability to dynamically create common understanding of network requirements, operations, and capabilities. Includes the ability to provide information on critical IT assets and potential cascade effects of failures on essential mission functions. Provides real-time analysis and reporting of mission impacts due to failures in network(s), applications, and services functionality and capability. Supports cyber-space analysis and cyber-battle assessment.	A4.2.1 Manage IE Situational Awareness	NOAP 02 NOAR 06 NOAR 07	S2.2.3 Cryptography Management Services S2.2.1 Security Metadata Management Services S1.2.3 Directory Management Services

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
Automated Configuration Changes	The ability to automatically disseminate and implement configuration changes to networks, data assets, services, applications, and device settings in conformance with standard configuration processes.	A1.1.2.1 Develop NetOps Policy A1.1.2.8 Develop Configuration Management Policy A2.1.2.1.2 Enable Access Controls A2.3.2 Manage Network Resources to Defend IE A2.6.2.3 Provide Operational Management of IA A3.2.1.2.1 Provide Self-Managing Computing Infrastructure Operations A3.2.1.3.2 Provide Optimization / Performance Controls A4.2.3.4 Provide Configuration Control	NOAR 05	S1.2.1 Access Control Services S2.2.2 Information Assurance Management Services S2.1.1 Change Management Services S1.2.3 Directory Management Services

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
Dynamic Configuration Management	The ability to prioritize and adjust IE resources to meet user demands and match dynamic shifts in requirements. This capability prioritizes infrastructure services (bandwidth, network operations, enterprise applications, etc.) based on mission needs.	A1.1.2.1 Develop NetOps Policy A1.1.2.8 Develop Configuration Management Policy A2.3.2 Manage Network Resources to Defend IE A2.6.2 Provide Policy-Based Management of IA Components of IE A3.2.1.3.2 Provide Optimization / Performance Controls A3.2.1.5 Provide Information on Computing Infrastructure Resources A3.2.1.3 Provide Computing Infrastructure Controls A4.2.3.4 Provide Configuration Control A4.2.3.6 Perform Patch Management A4.3.2 Develop NetOps Plans	SIP 03 NOAR 05	S1.2.3 Directory Management Services S2.1.1 Change Management Services
Dynamic Routing / Policy-based Management	The ability to implement and use dynamic routing / policy-based management to enable dynamic operation and management of the IE.	A2.6.2 Provide Policy-Based Management of IA Components of IE A3.2.1.3.2 Provide Optimization / Performance Controls	NOAR 05	S1.2.3 Directory Management Services S2.1.1 Change Management Services
End-to-End Quality of Service	The ability to proactively monitor and control service levels and quality of service on an end-to-end basis. End-to-end monitoring and control will be integrated across networks, computing platforms, systems, applications, and services.	A1.1.2.3 Develop Quality of Service (QoS) Policy A3.2.1.2.7.6 Assess Computing Infrastructure Requirements and Performance A3.2.2.4.1 Provide Quality of Service Mechanisms	SAR 03 CIR 04 CIR 05	
Integrated Network Operations Services	The ability to implement capabilities required to provide integrated network operations for the DoD IE. Integrated Network Operations provides for information access by any user across any network and security domain.	A4.2 Exercise Operational Control of IE Through NetOps A4.3 Plan IE NetOps	NOAR 01 NOAR 02 NOAR 03 NOAR 05	S1.2.3 Directory Management Services

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
NetOps-Enabled Resources	The ability to manage each IE resource so it provides data on its operational states, performance, availability, and security construct in an automated fashion to enable enterprise-wide situational awareness of the network for performance management purposes.	A3.2.1.3 Provide Computing Infrastructure Controls	GP 04 NOAR 06	
New Technology Implementation	The ability to identify, evaluate, test, and employ new technologies across the infrastructure. This capability allows the replacement or retirement of non-standard equipment types / sets and their associated support requirements with newer and broader-based technologies for an interoperable infrastructure. It includes the performance of comprehensive testing of new technologies before their deployment / implementation.	A3.2.1.1 Implement Joint Computing Infrastructure A3.3.1 Evolve Computing Infrastructure A3.3.2 Evolve Communications Infrastructure A4.2.3.5 Perform Tech Refresh	CIRP 04	S2.1.3 Common Development Platform Services S2.1.2 Virtual Test Platform Services
<b>Defend</b>	<b>The set of capabilities that ensure data and services are secured and trusted across DoD.</b>			
Cross Domain Security (CDS) Enforcement	The ability to conduct secure information exchange across domains that are protected at varying levels of security (up to and including the SCI classification level).	A1.1.2.7 Develop Information Sharing Policy A2.1.3 Provide Federation A2.2 Enable Cross Domain Security A3.1.1.3.2.1.1 Provide Directory Federation A5.2.1 Post Information	SAR 01 SAR 06 OPR 03	S1.3.2 Information Sharing Services S1.3.2.2 Cross Domain Services
Hardware and Software Vulnerability Assessment	The ability to evaluate hardware and software vulnerability to threats, both internal and external.	A2.3.1.1 Provide Technical Protection Standards A2.3.3 Provide IT Platform Protection A2.3.5 Manage Information Assurance & Vulnerability Assessment (IAVA) Compliance A4.2.4.1 Provide Security Monitoring, Vulnerability Analysis, and Threat Identification	SAR 05	S2.2.2 Information Assurance Management Services

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
IE Operations Threat Assessment	The ability to determine and analyze threats and risks associated with day to day operation of the IE. This capability evaluates events to determine those that are actual threats. Identification of threats will include specific information about the threat to facilitate response decisions.	A2.1.4.1 Define Threat Level A2.1.4.3 Identify Threats A2.3.2 Manage Network Resources to Defend IE A4.2.4.1 Provide Security Monitoring, Vulnerability Analysis, and Threat Identification A4.2.4.2 Perform Threat/ Incident Management	SAR 03 SAR 05	S2.2.2 Information Assurance Management Services
Supply Chain Risk Assessment	The ability to determine and analyze threats and risks associated with the supply chain for software, hardware, and services to enable DoD program, security, and operations personnel to understand the level of trust that can be associated with the IT components they acquire, manage or use. This capability also evaluates supplier vulnerability to threats internal and external.	A2.8.4 Evaluate Supplier Assurance A2.9 Manage Globalization Risks	SAP 02 SAR 05	S2.2.2 Information Assurance Management Services
Data and Metadata Protection	The ability to protect the integrity of data and metadata in transit, in storage, and during processing. In particular, this capability provides for confidentiality, integrity, and authorization of any information. It provides for encryption of all traffic from edge-to-edge, with traffic in the clear being unnecessary, unless demanded. The communications infrastructure further provides for exchange of information across domains operating at various security levels.	A1.1.2.9 Develop IA Policy A2.3.4 Enable Data Protection A3.1.3.1.2 Manage Integrity A3.2.1.2.9 Provide IA for Computing Infrastructure	GP 05 SAR 01 SAR 06 SAR 08 CRR 03	S2.2.1 Security Metadata Management Services
Network Defense	The ability to defend network infrastructure against known and postulated attacks and against new threats that have not previously been seen, while reducing network vulnerabilities. This includes defense against both kinetic and cyber attacks.	A2.3.1 Protect Network and Enclave Boundaries A2.3.2 Manage Network Resources to Defend IE A2.6.1 Manage Computer Network Defense (CND) and IA Services A4.2.4 Conduct Network Defense	SAR 01 SAR 03 SAR 04 NOAP 01	S2.2.2 Information Assurance Management Services

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
Sensitive / Classified Information Management	The ability to monitor and control or restrict access to sensitive or classified information by cleared persons having the need to know, and prevent unauthorized transfer of sensitive or classified information across networks operating at different classification levels. This capability also monitors cleared personnel to ensure they are not abusing their authorities.	A1.1.2.9.2 Develop Identity Management and Authentication (IdM&A) Policy A1.1.2.9.3 Develop Access Control Policy A2.1.4 Monitor Authentication and Access Control	DSDR 01 SAR 07 SAR 08 OPR 06 OPR 13	S3.2.1 Digital Access Policy Management Services S1.2.1 Access Control Services S1.2.2.2 Identity Management Services S1.2.2.3 Attribute Management Services S1.2.2.1 Authentication Management Services S1.2.3 Directory Management Services S2.2.1 Security Metadata Management Services
IE Incident Response	The ability to rapidly and securely respond to incidents threatening IE operations.	A2.1.4.1 Define Threat Level A2.1.4.3 Identify Threats A2.6.1 Manage Computer Network Defense and IA Services A4.2.2 Respond to IE Situation A4.2.4.2 Perform Threat/ Incident Management	SAR 03	
<b>Govern</b>	<b>The set of capabilities providing processes, policy and standards, and oversight of the development, deployment, use, and overall management of the IE.</b>			
<b>Processes and Models</b>	<b>The set of capabilities providing procedures and tools to be used for analysis enabling effective overall management of IE development, deployment, and use.</b>			
Architecture Development and Use	The ability to develop and use architectures to guide and constrain the development and implementation of the IE.	A1.1.1.2 Determine Common Infrastructure Architecture Requirements		
Best Practice Use	The ability to determine and use best practices derived from the Federal Government, industry, academia, and other members of the net-centric community in developing and implementing the IE. This requires DoD to partner with industry, Federally Funded Research and Development Centers (FFRDC), and academia to identify and generate innovative net-centric data and services solutions for information sharing challenges, and to participate in federal information sharing, open government, and transparency initiatives to improve information sharing with mission partners and the public.	A3.2.1.2.1.4 Provide Autonomous CI Environment A3.2.1.2.8 Provide COCOM Aligned Service Centers A4.2.4.2 Perform Threat / Incident Management		

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
Service Expense Sharing	The ability to develop new funding approaches that accommodate shared expenses between information providers and consumers. This involves "Budgeting" and it should be considered in budgeting processes.	A3.1.1.1 Provide Services Infrastructure	GP 04 DSDP 01 DSDR 02	
<b>Standards and Policy</b>	<b>The set of capabilities providing patterns and strategic direction to be followed to ensure interoperability across DoD.</b>			
Standard Protocol Management	The ability to establish and enforce standard protocols to provide information transmittal and acknowledgement across the DoD IE. This capability ensures the necessary tools and expertise are available to send and receive information, with the appropriate standard protocols for both information exchange and receipt acknowledgement.	A1.1.3.3 Develop Communications Standards A2.3.1.1 Provide Technical Protection Standards A3.2.2.1 Procure Interoperable Transport Components	GP 02 OPR 11 OPR 19 OPR 20 OPR 24 OPR 28	
Standard Security Engineering Practices	The ability to develop and enforce standard security engineering processes. A standard, approved security engineering process is used to establish, document, and validate all networks, data assets, services, applications, and device settings controlling IA functionality.	A1.1.2.4 Develop Quality of Protection (QoP) Policy	SAR 09	
Standardized IE Education and Training	The ability to provide standardized education and training of IE operators and users on essential processes, procedures and resources. Standardized education and training (to include NetOps, Security, and SOA training) will continuously develop knowledge and skills to support and enhance the abilities of individuals and teams performing IE functions. Standardized education and training will enable joint planning, simulation processes, shared lessons learned, and the ability to adjust cultural attitudes to enable the sharing of information more widely.	A1.1.1.7 Develop Joint Training Strategy A2.5.3 Oversee DoD IA Training and Education A5.3 Maintain IE Proficiency	SAR 04 NOAR 04 OPR 25 OPR 31 OPR 36	
Standard Guidance	The ability to establish and maintain a common set of enforceable policies and standards for the IE. Common policies and standards are written and enforced to ensure DoD networks and systems are integrated and provide seamless end-to-end information services to authorized users and mission partners. These policies and standards address user access and display devices and sensors, networking and processing, applications and services, and related transport and management services.	A1.1.2 Develop IE Functional Policy A1.1.3 Establish IE Standards	GP 02 SAR 02 NOAR 04 OPR 04 OPR 22 OPR 24 OPR 25 OPR 26 OPR 36	
Digital Policy Management	The ability to create and manage digital policies used to enable rapid modification of access, resource allocation, or prioritization (e.g., bandwidth, processing, and storage) through enterprise-wide, policy-based management in response to changing mission needs or threats.	A2.1.5 Manage Digital Rules		3.2.1 Digital Access Policy Management

Capability Descriptions

Name	Definition	Aligned Activities	Aligned Rules	Aligned Services
<b>Monitoring and Compliance</b>	<b>The set of capabilities enabling effective oversight of development, deployment, and use of the IE.</b>			
Oversight of IE Implementation	The ability to govern and oversee development and implementation of the IE. This capability provides for central governance of the development, acquisition, and fielding of IE capabilities; uses architectures in the governance and oversight process; and establishes technical, operational, and programmatic oversight and governance for common services at the enterprise level. Unity of command is provided for planning, resourcing, and operation of networking and information services, to include training and staffing requirements. A single authority is appointed for IE capabilities and to align forces and resources to support these capabilities.	A1.1.1 Develop IE Vision and Strategy A1.2 Implement Joint / Enterprise Level Governance of the IE	OPR 34 OPR 35	
Authoritative Body Identification / Empowerment	The ability to identify and empower authoritative bodies (e.g., COIs) to establish and implement the framework (methods, policies, procedures, and language) for sharing DoD data and resources.	A1.1.2.7 Develop Information Sharing Policy A3.1.3.2.1 Manage Communities of Interest (COIs) A5.2.2 Collaborate	DSDP 04 DSDR 05 DSDR 08	
National Green IT Initiative Implementation	The ability to implement national Green IT initiatives, as applicable.			
Infrastructure Certification and Accreditation	The ability to use standard processes and common policy to accredit, certify, and approve infrastructure across the IE.	A1.1.2.9.1 Develop IA Certification & Accreditation (C&A) Policy A2.4 Manage IE Certification and Accreditation (C&A) Program A3.2.1.2.7.6 Assess Computing Infrastructure Requirements and Performance	CIR 07 SAR 09 OPR 27	