



Surety

Reach

Speed

DISA

MARCH 2007

SURETY, REACH, SPEED

THE DISA STRATEGY

Second Edition



DEFENSE INFORMATION SYSTEMS AGENCY

The is the second edition of the DISA Strategy.
It adds clarity to several initiatives, and it emphasizes
defense of the Global Information Grid.

The DISA Strategy is a living document that will reflect
the evolution of our vision, mission, and challenges.
Updates to the strategy will be made regularly as part
of this evolution.

VISION

The Department of Defense vision for net-centric operations and warfare:

“The National Defense Strategy clearly states how we will operate in the future – we will be net-centric. Our job is to deliver the critical enabling capability to conduct network-centric operations.”

“Defense transformation hinges on the recognition that information is our greatest source of power. We can leverage information to allow decision makers at all levels to make better decisions faster and sooner.”

— *John G. Grimes, Assistant Secretary of Defense for Networks and Information Integration, and DoD CIO, March 2006*

We at DISA imagine and envision a world in which information is virtual and on demand with global reach. Information is protected by identity-based capabilities that allow users to connect, be identified, and access needed information in a trusted manner. It is a world in which United States military forces can deploy and connect no matter where they are located, pull information needed for their missions, and be given timely, accurate information on any threats they may face. It is a world with no seams between the sustaining base and the tactical edge so that operational agility is enabled. It is a world in which the United States military can freely exchange information routinely with coalition partners and others responsible for the security and defense of the United States. The technology employed is agile, adaptive, and capabilities-based. And, we imagine and envision a world in which our soldiers, sailors, airmen, and marines are equipped with capabilities and services that are state-of-the-art.

The Defense Department's Global Information Grid (GIG) will be a web-like enterprise in which people can discover information, orchestrate their own operational picture based on the situation at hand, have shared situational awareness, and operate securely. We will provide Internet technology at speeds necessary to bring people together efficiently, help them do their jobs in ways never anticipated, and enable them to do things never envisioned.


DISA must aggressively lead in five areas:

- Speed – deliver IT capabilities and services faster
- Power to edge – extend enterprise services to the edge
- Operational excellence – accelerate operational effectiveness and efficiency
- Sharing and defending information – enables sharing of information while staunchly protecting it
- Best value – customers know and understand the value of DISA capabilities and services

The “we” at DISA is our people – our most valuable asset. DISA will continue to recruit, develop, and professionalize the workforce to lead DoD in achieving net-centric operations.

A handwritten signature in black ink that reads "Charlie Croom". The signature is written in a cursive, flowing style.

Charles E. Croom, Jr.
Lieutenant General, USAF
Director



**How do we enable
warfighters at
Internet speed?**



**We will increase
the delivery speed
of capabilities and
services**

VISION AND STRATEGY

We will become the joint acquisition agent of choice for enterprise information technology capabilities and services. We will adopt innovative ideas and processes to deliver capabilities and services that our forces are able to use with agility.

We will increase the speed and flexibility of the requirements and acquisition processes used in delivering capabilities and services, and we will tailor oversight and governance to be commensurate with risk. Our goal is to close the gap between the availability of technologies and fielding them for warfighting advantage.

DISA will follow the precepts of adopt-before-we-buy and buy-before-we-create. If another organization has developed or acquired a capability or service that either fits or is close to fitting a need we have, we will adopt it. Where adoption opportunities are not available, we will turn to the private sector and acquire a capability or service that either fits or is close to fitting the need. The final choice is to create or build. We intend to avoid development and turn to others for solutions when we can.


Speed of deployment is often more important than a perfect solution. We will pursue the adopt-before-we-buy and buy-before-we-create approach partly as a way of getting the 80-percent solution in the hands of the warfighter quickly.

A fundamental element of our strategy is teamwork – teamwork with stakeholders, customers, and vendor partners. We will use a federated development and certification environment (FDCE), the “sandbox,” in which all can participate to foster innovation and collaboration and to introduce new capabilities and services into the GIG. We will ask developers, testers, and users to play in the “sandbox” by exposing candidate capabilities and services to warfighting, intelligence, and business users via the FDCE. We will incentivize vendors to do the same. Some candidates will take off; some will not. Success of the FDCE is dependent in part on the ability to do an early kill of those that do not. In any case, this richly collaborative approach will bring the best and brightest to the forefront and help us to speed the delivery of capabilities and services to warfighters.


INITIATIVES

Speed

- Employ innovative approaches to exploit the flexibility in the acquisition process.
- Change the way the DoD acquires IT to deliver capabilities and services at speeds commensurate with the Internet.
- Tailor governance and oversight commensurate to the level of risk.
- Aggressively exploit competition.
- Use performance-based approaches such as statements of objectives as a principal acquisition tool in lieu of detailed specifications.
- Use service level agreements to define performance expectations.
- Use the FDCE, pilots, proofs of concept, and experiments to determine if candidate capabilities and services are suitable, can scale, and can operate in appropriate security and operational environments.
- Ensure early and continuous involvement of Combatant Commands, Services, and Agencies and other communities of interest in sourcing decisions.
- Maximize the use of on-demand delivery of bandwidth, processing, storage, and web services, leveraging commercially available offerings.
- Develop innovative relationships with industry partners for strong performance-based solutions, speed, risk balance, and mission assurance.



**How do we enable
warfighters to get the
right information at
the right time?**



**We will extend
enterprise services
to the edge**

VISION AND STRATEGY

Warfighters must have access to timely, relevant, and accurate information anywhere, anytime. Success depends on the right information being available and usable by commanders at the right time. Therefore, it is no longer sufficient for DoD components to provide segments of the network that are independently developed and managed if these conditions are to be met. DISA will synchronize and integrate efforts with our partners to bring coherence to the network and extend DISA-provided capabilities and services to the edge.

This translates into the need for enterprise wide systems engineering, a common strategy and architecture, a single concept of operations for network operations, configuration control, and situational awareness that comprehensively spans the sustaining base to the tactical edge. The Enterprise Information Environment (EIE) provides standards, rules for data accuracy, the framework to place data on the network, and governance of information on the network. As the foundational element of the EIE, Net-Centric Enterprise Services (NCES) supports all mission areas and provides enterprise services to integrate the warfighter, business, and intelligence mission areas.

The Department must transform spectrum management, transitioning legacy processes and capabilities to support net-centric operations and warfare. DoD's spectrum access, when and where needed, is vital to the deployment, employment, and sustainment of a warfighting force anywhere in the world.

INITIATIVES

Enterprise Information Environment (EIE)

- Publish a set of technical procedures and standards to provide an enterprise wide design pattern for service and capability developers to ensure interoperability of independently developed IT capabilities.
- Establish a center of excellence for service oriented architecture (SOA) to lead SOA implementation in DoD.
- Migrate proprietary application interfaces and legacy information technology architectures to a SOA foundation, based on open web-services standards including loosely coupled core enterprise services.
- Develop criteria with clear metrics for accepting new capabilities and services identified in the FDCE onto the network.
- Implement a joint enterprise directory service and produce interoperability standards for enterprise directory data and metadata.
- Enable the DoD data strategy by publishing naming conventions, schemas, interface specifications, tools, and interoperability and performance standards.
- Ensure that all appropriate DISA internal systems are compliant with the DoD data strategy.
- Publish an extension of the EIE technical procedures and standards for DISA's internal systems.
- Develop the DISA SOA governance approach.

NetOps

- Deliver global capabilities and services to extend situational awareness and control of information across the sustaining base to the tactical edge.
- Establish policies and processes for information dissemination management (IDM) describing where and how data, capabilities, and services will be provisioned, stored, and managed on the network.
- Develop a process to achieve the capability to model information requirements in support of deploying warfighting forces and to execute content staging forward to support them.

Enterprise Wide Systems Engineering and Management

- Provide continuous oversight of the GIG's evolution.
- Maintain a GIG enterprise wide technical baseline.
- Establish enterprise wide analysis capabilities.
- Establish a GIG compliance management program.
- Establish and publish standards.

Spectrum

- Update the DoD Electromagnetic Spectrum Management Strategic Plan and develop the Defense Spectrum Management Architecture (DSMA) to guide the Department toward net-centric spectrum management.
- Develop a roadmap to achieve integration of the DSMA and the Global Electromagnetic Spectrum Information System into planning and execution.
- In coordination with NATO and other bodies, develop strategies to introduce dynamic spectrum access technologies and techniques, nationally and internationally.
- Develop enterprise wide capabilities to consistently investigate and integrate spectrum-efficient technologies into DoD systems.
- Develop efficient spectrum management processes using advanced technologies and techniques.

Terrestrial and Satellite Communications


- Migrate from circuit-based technology to a converged IP network and services environment in accordance with the GIG Convergence Master Plan.
- Implement quality of service and assured delivery capability for network and real time services and applications, with parameters that ensure proper end-to-end operations.
- Evolve to a single virtual DoD terrestrial and satellite communications

network providing capabilities and services from the sustaining base to the tactical edge.


- Provide responsive, agile, and cost effective commercial SATCOM services.
- Continue development of the DoD wireless strategy.

Scalable Net-Centric Computing

- Establish processes and an online mechanism for customers to directly provision a virtual operating environment on demand within minutes to meet ad hoc, real time warfighter needs.
- Establish a capability for applications to dynamically scale computing resources up and down on demand to meet traffic loads.
- Provide an enterprise level storage capability globally accessible to all DoD applications.
- Develop a common vocabulary and performance standards to describe a range of GIG Computing Nodes (GCNs) that can be used tactically.



**How do we
accelerate operational
excellence?**



**We will operate
effectively and
efficiently, lower costs,
and measure
quality of service**

VISION AND STRATEGY

The GIG is centrally operated, managed, and controlled in support of net-centric operations and warfare by the Joint Task Force-Global Network Operations (JTF-GNO). DISA is responsible for operating and sustaining the Defense Information Systems Network (DISN), the enterprise computing centers, enterprise services, and command and control capabilities and services.

Providing efficient and effective capabilities and services requires excellence in customer relationships and the agility required to adjust to dynamic requirements. We will partner with our customers and evaluate ourselves in terms of their success. We will simplify the business model for cost recovery of all DISA services. We will dramatically increase communication with our user community through improved web and web-services access and services status, and we will provide our customers with a feedback mechanism.

DISA's enterprise computing centers will be dramatically different in the future. Today, they are principally hosting environments for combat support applications in which customers pay for services either through rates or full cost recovery. While this model will continue, DISA's computing centers will also provide capabilities for rapid, just-in-time scaling of processing and storage to meet unanticipated needs for web services and other warfighting demands. Therefore, the enterprise computing centers must evolve technically and operationally and with business models that support the evolution.

We will structure NetOps capabilities to maximize operational effectiveness. We will implement enhancements to facilitate efficient provisioning, management, and cost recovery.

INITIATIVES

NetOps Optimization


- Continue development of the DoD NetOps architecture that includes standards, policies, and processes.
- Develop NetOps concepts to integrate telecommunications and computing service management to ensure timely access to and efficient use of information needed for mission execution, and optimize the NetOps centers to include continuity of operations to gain efficiencies.
- Automate the management and control of DISA elements of the GIG using machine-to-machine concepts and technology to reduce human intervention, improve availability and security, and reduce costs.
- Implement processes and procedures to support provisioning capabilities and services on demand.
- Standardize operations of DoD Teleports, Standard Tactical Entry Points, and other SATCOM gateways to ensure optimum management, use, and cost effectiveness.
- Standardize the operation of gateways between the GIG and the Internet – to include DoD Internet Access Points (IAP) and Demilitarized Zones (DMZs) – which enable protected and controlled access between the DoD and its partners.
- Establish the definitions, standards, and processes for service level management of DISA-provided capabilities and services.
- Develop criteria for DoD NetOps which address education, training, and certification of the workforce.

Network Evolution


- Transition from Asynchronous Transfer Mode (ATM) based services to Multi-service Provisioning Platform (MSPP) for physical circuits and Multi-Protocol Label Switching (MPLS) for the virtual circuit equivalent.
- Ensure the DISN is appropriately refreshed and expanded to provide improved security and to meet capacity demands.

Enterprise Computing

- Move toward the concept of virtual or grid computing in which applications will utilize available computing capacity irrespective of geographic location.
- Expand to provisioning and management of enterprise level storage capability ensuring data accuracy, integrity, and assurance.



**How do we make sure
that the warfighter
gets the right
information at the
right place and time?**



**We will aggressively
enable sharing of
information while
staunchly protecting it**

VISION AND STRATEGY

A warfighter's ability to leverage the right information at the right time is the difference between mission success and mission failure. We will provide state-of-the-art capabilities and services that enable sharing of information through an assured, accessible net-centric environment. These capabilities and services will enhance planning and execution of joint military and coalition operations in a responsive, agile, and cost effective manner. We will enable transition from a culture of need-to-know to one of need-to-share, while ensuring that the Department can still keep a secret when necessary. New sharing relationships will be built virtually and instantly.

We will aggressively develop and implement measures to manage and defend the GIG to ensure warfighting forces, including partners and allies, can deploy and connect globally, and share timely, trusted, and accurate information needed for their missions. We will design, implement, operate, and sustain the GIG for maximum mission assurance in the face of kinetic or cyber attack.

We will propose policy and implement instructions for security certification and accreditation supporting the fast paced, often ad hoc, on demand nature of net-centric operations and warfare. We must be able to add capabilities and services to the network at Internet speed.

INITIATIVES

Net-Centric Capabilities

- Deliver the Department's C2, combat service support, business, and intelligence capabilities using a net-centric, collaborative information environment.
- Publish an extension of the EIE set of technical procedures and standards for the C2 and combat service support, business, and intelligence communities.
- Provide standard coalition information sharing capabilities by combining the CENTRIXS, Griffin, and REL DMZ efforts and integrating them whenever possible with C2 and combat service support capabilities.
- Deploy cyber identity credentials throughout the GIG for safer and broader sharing.
- Continually assess the Public Key Infrastructure architecture for effectiveness.

NIPRNet and SIPRNet Hardening

- Redesign the NIPRNet and SIPRNet, including certain shared components (e.g., the domain name system), to dramatically enhance security and improve sharing.
- Develop and operate strengthened gateways between DoD and the Internet and between DoD, other United States networks, and coalition networks.


- With the Services and Agencies, plan and execute the movement of all publicly visible and partner-facing applications and services into DMZs to improve sharing and security.
- In coordination with other federal agencies and industry, provide security configuration guides, checklists, gold disks, and other standards to properly configure and manage applications, devices, and enclaves.
- Plan for, acquire, and deploy enterprise wide tools and capabilities that improve defense, attack sensing and reaction, and situational awareness.

Service Commissioning Process


- Develop and use a standard IA design evaluation and testing process for capabilities and services as part of the FDCE process.
- Develop policies and procedures for certification of organizations trusted and empowered to provide DoD certification and accreditation (C&A) of capabilities and services to be placed on the network.
- Develop and implement processes and procedures to ensure each capability and service placed on the network meets DoD data sharing, reliability, performance, and security standards.

Intrusion Detection and Diagnosis

- Develop and implement a DoD-wide intrusion and attack detection and diagnosis plan across all aspects of the delivery of capabilities and services.
- Develop a DoD-wide strategy for, and deterrence of, the insider threat.



**How do we make sure
that our customers
get the best, most
economical operating
capabilities?**



**We will be good
stewards, and we will
be efficient and open**

VISION AND STRATEGY

We will excel in our stewardship of taxpayer dollars through integrity, full and open financial disclosure, fiscal discipline, and professional competency. Success in these areas will lead to well-informed and accelerated investment decisions throughout DISA. We will attain a clean audit opinion.

Full financial disclosure is a cornerstone for attaining the highest standards of performance. With underlying comprehensive fiscal oversight, we are committed to lead and excel in the mutually supportive areas of cost visibility (open books), financial accountability, and fiscal discipline.

We will clearly link DISA-provided capabilities and services with their costs. This will allow customers and stakeholders to clearly see full value from every dollar in DISA-provided capabilities and services.

INITIATIVES

Stewardship

- Develop budgets that are compelling, defensible, consistent, and clearly aligned to support DoD priorities.
- Develop a metrics-based investment plan for use in the programming and budget processes that will allow practical evolution of capabilities and services over time.
- Improve metrics that forecast areas of potential weakness and track actual performance across the breadth of financial activities.
- Provide a simplified approach for customers to conduct financial business and share information with DISA.

Full Financial Disclosure

- Collaborate with OSD, the Defense Finance and Accounting Service, and others to implement a new financial accounting system and improved policies and processes.
- Ensure our internal processes are transparent so customers and stakeholders will understand our costs.
- Propose and explain cost recovery for DISA-provided capabilities and services such that our customers understand and accept their bills.
- Develop and track service metrics jointly with customers that reflect what is needed for their mission accomplishment.

Link Capabilities and Services to Cost

- Establish investment-based metrics that track use and cost of bandwidth, processing, and storage.
- Use clear and understandable costing mechanisms to establish fair and reasonable costs to customers, estimate costs effectively, deliver internal support services efficiently, and make informed resource allocation decisions.
- Define and measure cost drivers and manage those drivers to favorably affect the cost and content of our capabilities and services.
- Implement policies, procedures, and practices to ensure we are cost-based.

CONCLUSION

We at DISA believe information is the greatest source of military power. We, individually and collectively, can dramatically affect the future battlespace by ensuring U.S. and coalition warfighters can plug into the network and access and share information they need anytime, anywhere.

We are dedicated to delivering the power of information sooner and providing it across the enterprise to the tactical edge. We will assure its security, and we will ensure its provisioning is efficient, providing best value to the Department. We are dedicating ourselves to change where change gives us speed. We are dedicating ourselves to metrics where facts lead us to better decisions. We are dedicating ourselves to full and open financial disclosure and fiscal discipline for good, professional stewardship of taxpayer dollars.

This vision states how we will operate in the future and how we will move the Department closer to net-centric operations. In the end, providing information to the warfighter is a team sport – we will lead and we will partner – and we will remain faithful to the soldiers, sailors, airmen, and marines who rely on what we do to survive and win our nation’s wars.

Surety Reach Speed