



The Department of Defense Interim Information Assurance Strategic Plan

March 2008

Message from the DoD CIO

Defense transformation hinges on the recognition that information is one of our greatest sources of power. Information is a strategic component of situational awareness which enables decision makers at all levels to make better decisions faster and act sooner. Ensuring timely and trusted information is available wherever, whenever and to those who need it most, is at the heart of Net-Centricity.

Instead of “pushing information out” based on individually engineered and predetermined interfaces, Net-Centricity ensures that authorized users at any level can both “take what they need” and “contribute what they know.” However, these benefits of Net-Centricity unquestionably rely on one fundamental prerequisite: Information Assurance (IA). Users must have confidence that the information has integrity, authenticity and will be available when needed, and that the robustness and resiliency of the enterprise, even in the face of attack, will ensure that the mission can be accomplished. The threats to our information are real—they are multi-faceted, sophisticated and increasing daily. Today we have a “Defense-in-Depth” approach to assuring information—based largely upon firewalls and software patches—attempts to keep intruders out and data safe. Tomorrow, a “Defense-in-Breadth” approach is required to assure that our information capabilities and information critical components are trusted throughout their lifespan to achieve Decision/Mission Superiority.

The IA community’s challenge is to address today’s challenges while also developing new and innovative capabilities to avert and mitigate tomorrow’s threats. IA is an enabler of one of the most significant military transformations in more than 50 years. Significant progress has been made through the hard work, innovative thinking, and deep commitment of the IA community. However, much work remains to be done. This document re-affirms the IA Strategic Plan introduced in 2004 for assuring information and updates relevant objectives and the actions critical to securing the Net-Centric Global Information Grid (GIG) and achieving our long-term vision—*Deliver the Power of Information: Access – Share – Collaborate.*

Sincerely,

John G. Grimes

Message from the Deputy Assistant Secretary of Defense for Information and Identity Assurance

I am pleased to present this interim update to the DoD Information Assurance (IA) Strategic Plan, an update to the Plan we introduced in 2004. Our plan provides a solid foundation and framework for how we'll assure the Department's information. As stated in the original version of this plan, this is a living document and we're committed to updating it to ensure it remains a vital and accurate reflection of the major issues confronting the Department. As such, this update reflects the strategic priorities of the Department outlined in the QDR and the CIO's Strategic Plan and addresses the Deputy Secretary of Defense's emphasis on measuring performance based on outcomes. This plan calls out identity assurance as the foundation underpinning the Global Information Grid (GIG). It also places focus on achieving mission assurance by expanding the scope of our third goal, Providing Integrated IA Situational Awareness/IA Command and Control (C2), to leverage all elements of information warfare and operationalizing the *Defense-in-Breadth* approach.

The business and operational environments in which we operate continue to change daily. We cannot predict when or how today's technologies will be overtaken by more advanced technologies; nor can we predict how events around the world will affect future requirements and the costs to protect our assets. However, we can do our best to prepare for the impact of these external factors. In response to the management transformation to portfolio management, we've established the GIG IA Portfolio (GIAP) Management Office and organized our programs and initiatives under the IA Capability Portfolio. The IA Capability Portfolio is organized by the IA Capability Areas in the IA Component of the GIG Architecture which is directly aligned with the DoD Enterprise Information Environment Architecture (EIEA).

We will be conducting a complete review and revision of the plan this year. The updated plan will reflect this transformational shift and include clear, measurable, outcome-oriented objectives. The new plan will include our Integrated Performance Management Plan enabling us to measure our progress towards meeting these outcome-based objectives. It will also allow us to execute and comply with policy and implement the programs, projects and initiatives in the DoD IA Capability Portfolio by measuring and monitoring our program performance and operational compliance.

We are committed to ensuring our new plan reflects the dynamic environment within which we operate and will continue to deliver timely and trusted information.

Sincerely,

Robert Lentz

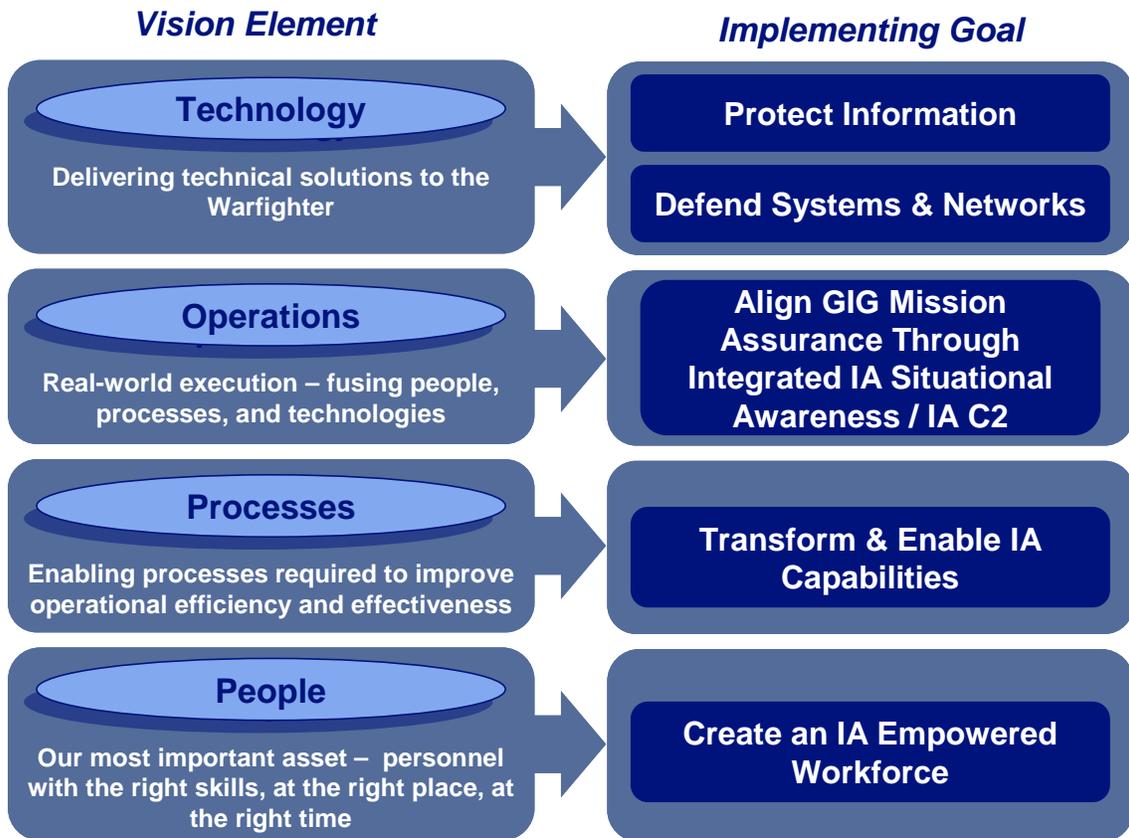
DoD Information Assurance (IA) Mission

Assure the Department's information, information systems and information infrastructure to support the Department's transformation to Network and Data-Centric Operations and Warfare and Global Information Grid (GIG) Mission Assurance.

DoD IA Vision

Dynamic Information Assurance for the GIG

To realize this vision we have defined five goals which lay the implementing framework to transforming our technologies, operations, processes and people:



These five goals and their supporting strategic and performance objectives are outlined in the sections that follow.

Our Technologies

- Minimize enterprise vulnerabilities while maximizing mission functionality
- Minimize adversaries' capabilities to exploit vulnerabilities through cutting-edge protection, identify assurance, detection and response technologies that are rapidly deployed across all DoD systems and networks

Our Operations

- Provide Warfighters and supporting personnel the confidence in the integrity and availability of information to achieve mission readiness
- Provide decision makers a seamless, enterprise-wide and common view of data to facilitate their collaborative decision making processes
- Allow sharing of information and knowledge throughout the GIG and enable multi-level information sharing across multiple security domains through our extended secure enterprise architecture
- Integrate non- DoD partners, as appropriate, into our operations
- Establish trusted networks and systems

Our Processes

- Meet Net-Ready criteria to support mission accomplishment in a Net-Centric environment and are continually improved to accommodate rapidly changing requirements and enhancements
- Improve cooperative relationships with academia, industry and research and development (R&D) organizations allowing for the development of mechanisms to foster rapid integration of state-of-the-art solutions and the use of assured hardware and software development processes in future IA capabilities
- Establish more effective and efficient validation, certification and accreditation of security processes and procedures across the enterprise
- Synchronize and effectively leverage all components of information operations

Our People

- Consistently demonstrate the highest skill levels in developing, managing and deploying the latest technologies and methods
- Recognize the importance of IA, understand its role, and are constantly vigilant.

Goal #1 – Protect Information to safeguard data as it is being collected, analyzed, processed and disseminated wherever to ensure all information has a level of trust commensurate with mission needs.

Assured information sharing is a national security priority. The goal of the GIG is to allow information originating from anywhere on the network to be available when needed throughout the network. Often the originator has little foreknowledge of who will use this information. The pace of events, National and Departmental objectives that place a priority on information, and the greater interconnectedness of organizations and with international partners are driving the move away from originator controlled “need to know” to a “need to share” with a corresponding “right to know” approach to information sharing. Therefore, the burden on IA is to ensure all information is protected from "end-to-end" and throughout its life cycle.

Data protection must start at the creation of the information, with particular focus on adding protection levels and access control parameters. Protection, trust and identity must be assured throughout the life cycle of the data: creation, modification, storage, transport and destruction. We can no longer rely simply on transport mechanisms such as link encryption to provide our end-to-end protection. Being part of a global network means that information (e.g., data, metadata) routinely flows in and out of the network through numerous access points. The separation of information from systems requires the protection of information, regardless of physical or logical location.

The DoD IA Architecture was designed to ensure information flow is protected throughout the enterprise, it aligns with the DoD Enterprise Information Environment Architecture (EIEA) that depicts the key DoD priorities of:

- Assured availability,
- Network Operations (NetOps) agility,
- Data and services deployment,
- Computing infrastructures readiness and
- Communications readiness.

The EIEA shows how IA is integrated with other DoD priorities. IA stovepipes and disconnects that prevent the warfighter from accessing needed information must be eliminated.

The roles of identity, authenticity, availability and confidentiality are critically important today. DoD has invested in programs such as Public Key Infrastructure (PKI), biometrics and Common Access Cards (CAC). However, more effort is needed for the integration and management of these identity technologies as well as to ensure these tools are implemented in a coordinated manner throughout the Department.

Coalition, cross-domain and collaborative communications require secure labeling and marking (“tagging”) of data for agile and dynamic access control decisions. Our supporting Security Management Infrastructures (SMI) (i.e., Key Management Infrastructure (KMI), PKI, and network management systems) must manage privileges for an attribute-based enterprise, support dynamic coalitions and be easy to use. They

must also have a higher level of assurance to protect the vital assets critical to the security of our protection mechanisms.

The plug-and-play protection envisioned for the future that will enable uniquely identified devices to be reconfigured for security or functionality purposes without human intervention must have strong authentication and authorization built in and make use of the SMI.

Achieving this goal of trusted data anywhere on the net requires partnerships and must be combined with the efforts of other members of the security community (i.e., physical security, personnel security and critical infrastructure protection) to provide an integrated systems security posture.

DoD's **strategic objectives** for this goal are to:

- Operationalize the GIG IA Architecture and the IA component of the DoD Enterprise Information Environment Architecture
- Develop and implement protection criteria for effective, Community-wide Net-Centric Operations
- Develop and deploy protection capabilities across the enterprise with increased focus on Mission Assurance
- Implement SMI to meet the agility demands of the end-state GIG with strong focus on Identity Management

Operationalize the GIG IA Architecture and the IA component of the DoD Enterprise Information Environment Architecture. The GIG IA Architecture provides the high level plan for IA across the enterprise. The results of this plan will increase interoperability and the compatible security solutions and ensure confidentiality, integrity, availability, authentication and non-repudiation throughout the enterprise and the National Security Community. The EIEA version 1.0 provides a common Enterprise Information Environment foundation to support accelerated DoD transformation to net-centric operations. It presents the vision of net-centric operations and establishes near term priorities to address critical barriers that must be overcome in order to achieve the vision.

Performance objectives. To support this strategic objective DoD will:

- Implement and enforce the end-to-end GIG IA Architecture and the EIEA
- Ensure the security engineering of all GIG acquisition programs is consistent with the IA Architecture
- Require compliance with an Enterprise-Wide IA/Computer Network Defense (CND) data strategy to guarantee seamless and timely sharing of mission critical information

Develop and implement protection criteria for effective, Community-wide Net-Centric Operations. Update IA policies to address the controls necessary to protect information and enable informed risk management decisions. Maintaining and revising

these policies, standards and criteria as technology progresses will allow implementation of secure solutions.

Performance objectives. To support this strategic objective DoD will:

- Implement the IA Policy Framework to satisfy “Net-Ready” needs
- Develop and evolve IA technical standards, criteria and implementation guides

Develop and deploy protection capabilities across the enterprise with increased focus on Mission Assurance. Our protective capabilities must continually evolve in response to the emerging threats and technological advances, to decrease the risk of information loss and operation compromise.

The application of protective mechanisms, integrated with sound system security engineering practices across the enterprise, reduces potential points of failure and provides consistency across multiple access points. Of paramount importance is to immediately improve information sharing across the enterprise and with our key partners to establish a vigorous end-state plan for multi-level information sharing and protection of critical program information.

Performance objectives. To support this strategic objective DoD will:

- Develop, improve and maintain robust, cutting edge, cryptographic capabilities
- Develop and provide enterprise service for identity and access management and cross domain/communities of interest exchange
- Support and enable information sharing via multi-level security domains
- Develop and implement data-at-rest protection techniques
- Implement enhanced security for the Secure Mobile Environment
- Expand the development and deployment of a modern cryptographic inventory through a COTS protection strategy to promote more effective information sharing with our key partners

Implement robust SMI to satisfy the agility demands of the end-state GIG with strong focus on Key and Identity Management. We must focus efforts on the SMI to support Net-Centric Operations, protect against cyber threats, both internal and external, identifying and differentiating between friendly and hostile forces and minimize impact to secure operations. Realizing a robust, usable security infrastructure that can respond on demand to changing technologies, capabilities, threats, alliances and coalitions is key to successfully defending against threats on the Net.

Performance objectives. To support this strategic objective DoD will:

- Build an identity assurance architecture that is consistent with the GIG and leverages federated capabilities
- Develop and implement robust key management capabilities (i.e., Key Management Infrastructure)
- Provide for assured authentication through implementing and using PKI and biometrics with all partners, including leveraging the Federated Enterprise
- Apply Net-Centric Operations to transform SMI

- Develop and implement attribute-based access control capabilities
- Expand assured identity services into the NIPRNet and SIPRNet

Goal #2 – Defend Systems and Networks by recognizing, reacting to and responding to threats, vulnerabilities and deficiencies and by ensuring all systems and networks are capable of self-defense.

DoD systems and networks are constantly under attack and must be continuously defended. To ensure success, defensive mechanisms must be an integral part of the design and implementation of systems and networks across the enterprise. In addition, capabilities must be deployed to react and respond to threats and attacks.

In a collaborative environment, defending the GIG requires expanded network and host-based defenses that will allow the network to:

- Identify, attribute, report and correct suspicious or unwanted behavior
- Automate system re-baselining to a known good state per INFOCON changes
- Detect and respond to the differences between legitimate and suspicious demands for system and network resources
- Identify and mitigate vulnerabilities

The principal points of focus for this goal are the CND protection, detection and reaction mechanisms for DoD systems and networks and adaptive configuration management. The time between vulnerability identification and exploitation has been reduced to the point that automated or semi-automated responses have become critical.

DoD's strategic objectives for this goal are to:

- Refine the GIG Network Defense capabilities to respond faster to known threats and vulnerabilities
- Develop and enforce CND policies across the enterprise to achieve an optimal readiness posture against the spectrum of attacks from “nation state” attackers to insider threats
- Evaluate and deploy CND tools and capabilities in a coordinated manner to achieve required operational capability
- Mitigate the insider threat across DoD through the implementation of advanced tools, processes and operational capabilities
- Develop and deploy a sophisticated and synthesized CND Enterprise Sensor Grid leveraging community-wide capabilities for proactive defense and response

Refine the GIG Network Defense capabilities to respond faster to known threats and vulnerabilities. Network and system components must be designed for IA and security and must be capable of being centrally managed and upgraded with new IA/security capabilities. Unfamiliar and complex system and network configurations cannot be adequately defended.

We cannot continue to operate with a patchwork of systems and networks that increase the warfighter exposure to vulnerabilities. Establishing a defensible enterprise network

architecture will provide the ability to manage complexity and provide evolving robust responses.

Performance objectives. To support this strategic objective DoD will:

- Refine the baseline GIG Network Defense capabilities and validate/harmonize with GIG Architecture
- Develop enhanced defensive capabilities and integrate these into the GIG architecture
- Support robust and flexible IA capabilities that secure any DoD/non-DoD architectures required for operations

Develop and enforce CND policies across the enterprise to achieve an optimal readiness posture against the spectrum of attacks from “nation state” attackers to insider threats. By laying the framework for operation and administration of network defense, the efforts from this strategic area help the warfighters effectively defend the net through clear guidance, consistency of operations and high readiness throughout the DoD enterprise.

Performance objectives: DoD will:

- Develop, promulgate and enforce enterprise CND policies and guidelines
- Integrate exercises, risk assessments and Red/Blue Team assessments and results into operational requirements
- Establish and identify supporting initiatives and assessments

Evaluate and deploy CND tools and capabilities in a coordinated manner to achieve required operational capability. Constant vigilance is required to maintain and improve our ability to identify emerging threats and impending degradations. Failure to continuously assess and evaluate our systems and networks decreases our ability to detect and respond to threats prior to their negative impact. By deploying CND tools and capabilities across the DoD enterprise in a coordinated and consistent way, it will mitigate risk of a “weak link” organization and enable desired operational capability on a Departmental level.

Performance objectives. To support this strategic objective DoD will:

- Deploy standard vulnerability and configuration management tools across the enterprise
- Deploy anomaly detection, threat prediction and analysis capabilities
- Deploy expanded intrusion detection and data correlation tools and capabilities
- Implement demilitarized zones (DMZs) across the GIG

Mitigate the insider threat across DoD through the implementation of advanced tools, processes and operational capabilities. DoD realizes the importance of protecting its systems and networks not only from untrusted outsiders, but also from the trusted insider. DoD will leverage other CND initiatives, including policies and tools to respond and effectively manage insider threats.

Performance objectives. To support this strategic objective DoD will:

- Deploy specialized tools aligned with policies, processes and techniques to mitigate the threat
- Continuously monitor the enterprise to assure improvement and make necessary adjustments
- Refine planning guidance for the POM cycles and develop initiatives to mitigate the insider threat across DoD

Develop and deploy a sophisticated and synthesized CND Enterprise Sensor Grid leveraging community-wide capabilities for proactive defense and response.

Enterprise level IA requires the capability to analyze sensor data horizontally and vertically within the entire DoD enclave. The Enterprise Sensor Grid (ESG) will pull information, raw and analyzed, from the CND tools and capabilities deployed in Goal 2 into a cohesive DoD-level system. The ESG will enable information fusion of technical CND data contributing to larger CND Indications & Warning (I&W), NetOps, and Computer Network Operations (CNO) efforts.

Performance objectives. To support this strategic objective DoD will:

- Develop policies, processes and procedures for information sharing from enterprise-wide CND sensor capabilities
- Continue advancement of the Attack, Sense and Warning (AS&W) capability and other anomaly detection and analysis capabilities for integration into the ESG and supporting enterprise I&W efforts
- Expedite delivery of the ESG to enhance IA support to GIG Bandwidth Expansion

Goal #3 – Align GIG Mission Assurance Through Integrated IA Situational Awareness/IA Command and Control (C2) integrating the User-Defined Operational Picture (UDOP) synchronized with NetOps and emerging GIG Common Operating Picture (COP) programs to provide decision makers and network operators at all levels the capabilities for conducting IA/CND operations in Net-Centric Warfare (NCW).

The complex and interdependent nature of our information networks and the demands of NCW require shared awareness and understanding across the enterprise to enable effective C2. Combatant Commanders require sufficient visibility into their network operations that includes situational awareness regarding the threats to these networks and the IA capabilities. To meet this need, the IA community must work closely with Combatant Commanders, Services and Agencies to identify IA Situational Awareness/C2 requirements and build and deploy the capability to meet these requirements.

DoD's strategic objectives for this goal are to:

- Establish effective CND I&W of potential or ongoing attacks against the enterprise and with key partners
- Develop and deploy a CND UDOP integrated with evolving NetOps and GIG COP capabilities

- Conduct near-real-time and integrated IA and NetOps decision making across the enterprise
- Harmonize NetOps and CNO policies, doctrine, relationships and operations
- Establish mechanisms and procedures within CND response action guidelines that effectively utilize deployed CND tools and capabilities
- Achieve Mission Assurance through the coordinated execution of GIG continuity of operations and resiliency planning

Establish effective CND I&W of potential or ongoing attacks against the enterprise and with key partners. Protection of our networks must be a proactive process using all available information on threats to known and suspected vulnerabilities. Threat information ranges from strategic level information on nation-states' and non-state actor's capabilities and intentions to near-real-time tactical information on computer probing activities preparatory to an attack. It includes information from traditional intelligence, counterintelligence and open sources, as well as information from worldwide law enforcement, computer emergency response team and government and industry technical sources. Analysis of this information requires the collaboration of intelligence, operations and technical organizations and personnel. Furthermore, as decision cycles are generally extremely short, rapid distribution of this analyzed information is critical to identifying potential threats to the enterprise to warn commanders and enable appropriate defense and response options.

Performance objectives. To support this strategic objective DoD will:

- Define the process and establish policies and procedures for CND I&W and rapid dissemination of warning information within DoD and to interagency and international partners
- Integrate relevant and timely Intelligence and Enterprise Sensor Grid data and analysis, and industry, law enforcement, interagency, international military and worldwide computer emergency response team information into the CND I&W process

Develop and deploy a CND UDOP integrated with evolving NetOps and GIG COP capabilities. Net-Centric Warfare demands shared awareness and understanding across the enterprise. A UDOP of the networks, the missions these networks support and network IA status, provides commanders and network operators with greater flexibility and reduces the risk of negative impacts resulting from unilateral, uncoordinated actions. Interoperability between the CND UDOP and current/emerging common operating pictures at the Service, Joint, Combined and Standing Joint Force Headquarters (SJFHQ) levels further enhances the synergy between NetOps, IA and other military operations.

Performance objectives. To support this strategic objective DoD will:

- Identify IA/NetOps information requirements for inclusion in GIG COP, including:
 - Consideration of DoD and Allied/Coalition networks
 - Input from Interagency, Allied and Coalition partners
- Identify the "As Is" state of IA and NetOps situational awareness

- Integrate ESG and IA I&W capabilities into the UDOP
- Plan and build the “To Be” or objective CND UDOP ensuring interoperability and synchronization with COPs at the Service, Joint, Combined and SJFHQ levels

Conduct near-real-time and integrated IA and NetOps decision making across the enterprise. Decision making in isolation often results in unacceptable and unintended consequences. Improved coordination increases our ability to quickly identify, contain and respond to threats, thereby avoiding the transfer of risks.

Performance objectives. To support this strategic objective DoD will:

- Provide effective IA C2 and collaboration capabilities
- Improve, standardize and integrate CND and NetOps
- Establish timely IA reporting and notification procedures for the extended enterprise and with key critical infrastructure protection partners, including the Defense Industrial Base (DIB)
- Improve the INFOCON process and supporting modeling and simulation capabilities to better develop courses of action, reduce decision and execution timelines and evaluate effects across the enterprise

Harmonize NetOps and CNO policies, doctrine, relationships and operations.

DoD's networks are dispersed, autonomous, overlapping and interdependent entities. Many of these networks are not exclusively owned or controlled by DoD, but may be part of the larger Global Grid, Internet or Foreign government/military networks. Commanders and network operators must collaborate to ensure the integrity, confidentiality and reliability of the information for the Warfighter. Likewise, CNO, which includes the mission areas of Computer Network Attack (CNA), exploitation and defense, policies and doctrine must be coordinated with IA/NetOps activities to ensure the GIG supports DoD missions under all threats, both cyber and physical. Mission Assurance in support of the DoD leaders accomplishing assigned missions under all threat levels requires harmonious relations, cohesive doctrine and synchronized operations and policies with all organizations that share in their management and protection.

Performance objectives. To support this strategic objective DoD will:

- Implement proactive CND-Response Actions (CND-RA) policies and capabilities
- Assess and evaluate current and future collaboration efforts and command relationships to identify their operational impacts and coordinate policies and procedures to mitigate risk to DoD networks
- Establish active relationships with other governmental, academic, civilian, international and coalition agencies and organizations to provide critical data interchange
- Evaluate collaboration vulnerabilities and benefits to prioritize DoD efforts and mitigate risk

- Leverage CNO policy, doctrine and capabilities to support DoD Critical Infrastructure Protection (CIP) responsibilities

Establish mechanisms and procedures within CND response action guidelines that effectively utilize deployed CND tools and capabilities. Improved capabilities to attribute, react and respond to incidents and vulnerabilities reduce the risk of losing mission-critical capabilities. These response action procedures and processes must fit into the CND-RA framework for rapid and consistent enterprise responses.

Performance objectives. To support this strategic objective DoD will:

- Deploy rapid and enhanced forensic support and system administrator capabilities to improve incident responses across the enterprise
- Identify and develop requirements and initiatives that will lead to enterprise automated threat recognition, reaction and reconstitution capabilities
- Enable enterprise-wide consequence management [cyber Standard Operating Procedures (SOPs) and Continuity of Operations Planning (COOP)]
- Establish standardized program reporting and response processes and procedures across all networks

Achieve Mission Assurance through the coordinated execution of GIG continuity of operations and resiliency planning. Executing missions in a Net-Centric environment demands that the Department have the ability to rapidly recover from any denial or degradation of the GIG that affects critical missions. We must deliberately build greater resiliency into the GIG so as to reduce the impacts and cascade effects of attacks and be prepared to operate with degraded or untrusted networks and to quickly reconstitute those elements of the GIG supporting our critical Mission Essential Functions (MEFs). Those critical MEFs are: 1) Advise the President; 2) Employ the U.S. Armed Forces; 3) Maintain Command Authority; and 4) Maintain Worldwide Situational Awareness.

Mission Assurance also requires that today's concepts for operating and defending the GIG be broadened to address the C2 structures and processes for reconstituting GIG capabilities that have been interrupted. Effective C2 would depend on a GIG-wide situational awareness derived from the combination of real-time network status and knowledge of pre-existing vulnerabilities, dependencies and cascade effects to the DoD MEFs.

Performance objectives. To support this strategic objective DoD will:

- Plan for worst case scenarios, by training and exercising under sophisticated cyber attacks
- Achieve mission resiliency by improving our Networks & Continuity of Operations
- Command and Control the GIG for mission success by enhancing governance of to support Mission Assurance
- Collect and analyze knowledge of adversaries' capabilities and intent by enhancing integration with the Intelligence Community

Goal #4 – Transform and Enable IA Capabilities through innovation and experimentation, leveraging emerging technologies, operationalizing IA best practices and refining foundational processes to improve cycle time, reduce risk exposure and increase return on investments.

The ever-changing and evolving information technology industry stresses DoD's processes and challenges them to keep pace. To maintain a competitive edge over our adversaries we must transform the way we develop and deliver new and dynamic capabilities to become more responsive to ever-changing needs. We must be agile and continuous improvement is critical.

Net-Centric Operations demand greater process agility and integration. We must rethink and innovate our planning, programming and resourcing processes in order to bring newly effective emerging ideas to warfighters in time to make a difference. We must rapidly respond to ideas that take root and come to market in time frames faster than current processes can recognize. We must transform how we conduct business among ourselves as well as across traditional boundaries.

Transforming IA capabilities depends heavily on the processes the Department uses to create, assess, test and implement new ideas. Developing new approaches to problem solving depends on the synergy between each process as the idea progresses from concept to reality. The focus of this goal is to influence the development of three key processes: innovation, planning and acquisition so they better serve the IA mission and thereby, a more agile force.

DoD's strategic objectives for this goal are to:

- Ensure that IA is integrated and sustained throughout the lifecycle of all DoD programs
- Improve the quality of strategic decision making, IA governance and portfolio management
- Expedite the development and delivery of dynamic IA capabilities through innovation
- Manage risk and enable efficient information sharing and collaboration across traditional boundaries to reduce the impact of globalization

Ensure that IA is integrated and sustained throughout the lifecycle of all DoD programs. All DoD acquisitions today must acknowledge that security cannot be traded off lightly for added functionality. Program Managers (PMs) and commanders must understand IA provides critical capability for weapons, sensors and communication systems. Jointness, interoperability and IA are integral capabilities of any DoD system. Integrating IA requirements into DoD's business processes enables the pervasive and consistent implementation of IA across the enterprise. We must focus on program management to ensure IA is embedded at the start and sustained throughout a program's lifecycle.

Performance objectives. To support this strategic objective DoD will:

- Ensure IA is integrated and maintained as a priority within departmental processes (e.g., requirements, acquisition, planning, budgeting and execution)
- Ensure the IA strategy is developed and implemented as a major joint activity
- Leverage vulnerability assessments, lessons learned, exercise results to influence requirements
- Incorporate IA changes into the Defense Federal Acquisition Regulations to include emphasis on supply chain risk management

Improve the quality of strategic decision making, IA governance and portfolio management. Realizing the vision requires a concerted effort across the Defense IA Community. To improve the planning function for the IA community we must establish a shared vision with supporting goals, objectives and metrics that will help us prioritize, align and monitor our resources, investments and operations. Only through the cohesive efforts of the IA community can we produce community endorsed priorities to build the business case for the proper funding of much needed IA capabilities. Prioritizing, aligning and monitoring investments to achieve common goals will improve DoD's overall risk management and return on investment.

Performance objectives. To support this strategic objective DoD will:

- Maintain a shared vision, goals and objectives and implement a standardized strategic planning and management process across the enterprise
- Align enterprise-level investment priorities with strategy and the management of the GIG IA Portfolio
- Transform, communicate and implement effective IA governance and guidance
- Establish an enterprise level Integrated Performance Management Plan (IPMP)

Expedite the development and delivery of dynamic IA capabilities through innovation. Industry is the primary provider for many IA capabilities, and technology is evolving at break-neck speed. We must continue to position ourselves to take advantage of new, commercially available technologies in real time by establishing relationships with development companies, integrating R&D efforts to better understand where we need to invest in GOTS development, and improving transition time to provide for timely and affordable innovation. We must also improve our internal processes to develop and identify new ideas and concepts, conduct research and development and deploy cutting-edge capabilities to maintain a competitive advantage. Improving existing processes will reduce the rate of obsolescence and costs to sustain legacy capabilities.

Performance objectives. To support this strategic objective DoD will:

- Improve the management of the IA R&D portfolio
- Increase throughput of ideas for new and dynamic IA capabilities through improved relationships with industry and with a focus on supply chain risk mitigation
- Discover and expedite the transition of emerging IA technologies and concepts from non-traditional sources, including venture capital and academia

- Identify, review, test and evaluate technologies for experimentation, implementation or investment
- Improve programs and processes fundamental to implement COTS/GOTS solutions in a risk-managed way
- Transform the existing certification and accreditation process for IT/IA

Manage risk and enable efficient information sharing and collaboration across traditional boundaries to reduce the impact of globalization. Globalization of commercial information and communications technologies provides our adversaries increased opportunities to penetrate our supply chain to gain unauthorized access to data, alter data, or interrupt communications. A common understanding of risk must be established across the Department and Homeland and National Security communities and among organizations and enterprises, taking into consideration what missions or functions are important, how they might be impacted, and what happens if they are lost or compromised. A universally accepted risk assessment methodology will provide information and system owners with confidence that the risks associated with sharing their information over interconnected systems are mutually understood and accepted. In addition, users must determine acceptable levels of risk and work to mitigate and manage the risk introduced by acquired products and services.

In the face of increasing globalization and the increasing sophistication of adversaries, improved collaboration within the enterprise and with external entities, both internal and external to the U.S. Government, enables us to share the successes and mitigate the results of failures in a shared-risk environment. Robust partnerships with other Federal agencies, particularly with the Department of Homeland Security and the private sector in areas of common concern are critical to this sharing.

We must create a broader awareness, understanding and knowledge base within the IA community. Breaking down cultural and organizational barriers to sharing information and implementing enabling technologies are critical to assuring information in a net-centric environment. Extending the enterprise architecture will result in increased investment efficiency, improved interoperability, increased technological and skill diversity and decreased time needed to implement new capabilities.

Performance objectives. To support this strategic objective DoD will:

- Operate a common risk management framework to include supply chain risk mitigation with the National Security Community and other U.S. Government critical infrastructure partners, as necessary
- Develop a risk mitigation strategy to minimize the security risk to National Security Systems (NSS) stemming from the rapidly changing global environment
- Partner across government and with critical infrastructure sector, including the Defense Industrial Base (under the auspices of the Department of Homeland Security's Critical Infrastructure Partnership Advisory Council), for enhanced CND/NetOps
- Identify and mitigate policy and regulatory impediments to efficient information sharing with non-DoD partners

- Establish an enterprise IA portal to serve as the centralized access point to IA information across the enterprise
- Implement secure, robust, enterprise-wide collaboration tools
- Provide trusted digital identities for users and information within the DoD Enterprise that facilitates the dynamic pushing and sharing of information globally

Goal #5 – Create an IA Empowered Workforce that is well equipped to support the changing demands of the IA/IT enterprise.

People are critical to protecting the Department’s information and defending its information infrastructure. This includes both end users who use computer applications in the course of their daily work and personnel who perform IA technical and managerial functions. This goal focuses primarily on the latter and is intended to establish an IA professional workforce with the knowledge, skills and abilities to effectively prevent, deter and respond to threats against DoD information, information systems and information infrastructures. We must effectively manage the IA workforce to place people with the right skills in the right place at the right time.

This goal addresses IA awareness, technical training, security management, and professional education. IA awareness is targeted to all DoD employees, from entry level to Senior Executive Service (SES) and Flag Officer. Information Assurance Technician (IAT) training focuses on personnel performing IA functions on DoD workstations, systems and networks, as well as IA Managers (IAM), Designated Approving Authorities (DAA) and their IA staffs. Education programs provide IA/IT Managers and program and project managers with technical, management and strategic leadership skills required for critical IA management and infrastructure protection functions within DoD.

The strategic objectives listed below comprise the DoD IA Workforce Improvement Program (IA WIP). DoD’s strategic objectives for this goal are to:

- Establish baseline certifications across the enterprise
- Provide trained/skilled people when and where needed
- Continuously enhance IA skills to keep current with technology and threats
- Infuse IA awareness and concepts into other disciplines and other entities
- Establish means of measuring the effectiveness of program/process improvements

Establish baseline certifications across the enterprise. The Department’s current approach to certification is a Component level program. There is wide variation in training content, the depth and breadth to which topics are addressed and implementation across the Department. The objective is to define the baseline IA competencies that personnel with various IA responsibilities must possess in order to perform their particular IA functions. Due to the rapid pace of change in technology and associated vulnerabilities and threats, this strategic objective seeks to address standardization of baseline skills by leveraging existing commercial certifications.

Performance objective. To support this strategic objective DoD will:

- Establish an enterprise-wide IA/IT certification program
- Influence certification providers to better support the DoD IA workforce

Provide trained/skilled people when and where needed. Currently, the Department does not possess the management tools/databases to effectively or efficiently manage the IA Workforce at the enterprise level. Integrated enterprise databases sharing critical workforce data are critical to full compliance with the law and DoD policy. The focus of this objective is two-fold: first, develop appropriate tools that when populated will allow Components and Agencies to effectively manage their IA workforce; and second, identify IA billets and specify skill indicators for personnel who perform IA functions, regardless of occupational specialty or series or whether the function is performed on a full or part-time basis.

DoD must also leverage existing tools, such as specialty pay/bonuses, educational incentive programs and new approaches to foster recruitment and retention. Strategic use of the IA Scholarship Program (IASP) to recruit “Millennials” or “Net-Generation” workers and to retain the current DoD IA workforce are of paramount importance. This will require fully utilizing Centers of Academic Excellence (CAEs) such as the DoD-designated institutions (Air Force Institute of Technology, Naval Postgraduate School, and Information Resources Management College of the National Defense University), to educate IA/IT professionals; and use of visiting IA professors to enhance DoD schools.

Performance objectives. To support this strategic objective DoD will:

- Improve the management of the IA/IT workforce
- Improve the recruitment and retention of IA personnel
- Promote effective use of IASP and CAEs
- Promote the CAEs as primary sources of IA Education for DoD personnel

Continuously enhance IA skill levels to keep current with technology and threats. In light of the dynamic nature of the IT environment, it is critical to maintain and broaden the skills of personnel performing IA/IT functions on a continuous basis. This objective is to provide IA/IT professionals access to the training they need to keep current with tools, techniques, vulnerabilities, threats, policies and key concepts. All methods of training and education need to be leveraged, including community colleges, undergraduate and graduate schools, distributive training and formal classroom training through Service schools and/or vendors. Reliance on commercial certifications, which require periodic refresher training and/or testing, provides the impetus for IA/IT professionals to get the training they need to maintain current technical skills.

Performance objective. To support this strategic objective DoD will:

- Improve IA training life cycle management
- Foster more rigorous, hands-on IA technical training, simulation, and exercises
- Influence training vendors to better support DoD IA requirements

Infuse IA awareness and concepts into other disciplines and into other entities. To increase overall awareness, DoD must identify other disciplines and external entities that

need to know about IA. DoD has the responsibility under Presidential Decision Directive 63 to make its distributive products available to the federal workforce and to share best practices, standards and training tools with academia, industry, Allies and Coalition partners. DoD must provide IA training and awareness content for other disciplines to incorporate into their training and awareness programs. Acquisition, law enforcement, public affairs and legal are examples of such disciplines.

Performance objectives. To support this strategic objective DoD will:

- Share IA training and awareness products with external entities
- Incorporate IA content into other DoD training program curriculum
- Establish a DoD Information Security System Line of Business (ISSLOB) Tier 1 Awareness shared service center

Establish means of measuring the effectiveness of program/process improvements

To focus resources to improve the overall IA posture, the Department must be able to track program progress and be able to identify gaps and deficiencies to meet Federal Information Security Management Act (FISMA) requirements, the Department must be able to validate component personnel and training awareness program data.

Performance objective. To support this strategic objective DoD will:

- Develop a policy compliance review plan and checklist
- Collect performance data to measure program/process improvements

Road Ahead

This Strategic Plan provides a solid foundation and framework for how we'll assure the Department's information. This is a living document and we're committed to ensuring our new plan reflects the dynamic environment within which we operate and will continue to deliver timely and trusted information.

As previously stated, we plan on conducting a complete review and revision of the plan this year. The updated plan will reflect this transformational shift and include clear, measurable, outcome-oriented objectives. Successful planning and execution in support of the IA mission requires the involvement and commitment of all Combatant Commands, Services and Agencies and we look forward to working with the DoD Information Assurance Community in this important effort.