



**Executive Services Directorate
Information Management
Strategic Plan
FY 08 - 12**

1 October 2007

Prepared by

**Assistant Director for Systems and Services,
Executive Services Directorate,
Washington Headquarters Services**

TABLE OF CONTENTS

TOPIC	Paragraph	Page
Message from the Director		1
Executive Summary		2
Section I - Introduction		
Purpose	1-1	3
Scope	1-2	3
Applicability	1-3	3
Plan Organization	1-4	3
Responsibilities	1-5	3
Section II – ESD Vision and IM/IT Tenets		
ESD's Mission, Vision and Goals	2-1	4
ESD IM/IT Vision	2-2	6
IM/IT Tenets	2-3	7
IM/IT Decision Principles	2-4	8
Section III – Strategies		
Full Cycle Governance	3-1	9
IM/IT Governance Components	3-2	10
Section IV – Goals		
Two years out--FY 08-09 Goals	4-1	13
Three and four years out--FY 10-11 Goals	4-2	15
Five years out—FY 2012	4-3	15
Summary		16
Appendices		
Appendix A – Definitions		17
Appendix B - Regulatory Guidance and Related Publications		20

Message from the Director

Executive Services Directorate is entrusted with a myriad of tremendous and critical missions in support of the Secretary of Defense and his senior leaders who bear the responsibility for the security of our Nation. We are able to fulfill these consistently in a professional manner. ESD is a great organization, recognized for being responsive, reliable, and relevant. But, we cannot and should not be content with whom and what we were yesterday and who and what we are today. If we are, then we risk becoming stagnant and losing the edge. It is the responsibility for each of us to not only do our best every day, but also to seek opportunities to make improvements to our business processes and tools along with our customer service, to stretch ourselves, and to contribute to making ESD a better organization in which to work and serve.

In discussing "continuous transformation" in the March 2006 National Defense Strategy, Secretary of Defense Donald Rumsfeld emphasizes that "...transformational change is not limited to operational forces. We also want to change longstanding business processes within the department to take advantage of IT." Information Technology (IT) is fundamental to our success as a directorate and leveraging its capabilities allows us to expand the critical role ESD plays in supporting the Secretary and Deputy Secretaries of Defense and OSD Components.

Technology is a critical enabler to all that we do, but tight resources require us to make the hard decisions – ensuring that priority is given to technology that is critical to our mission accomplishment, balanced against the need for innovation. ESD will continue to implement innovative IT initiatives while upgrading information technologies, improving security, and providing enterprise solutions to enhance mission accomplishment. We will review processes and develop teams, procedures, and tools to improve our work environment. We will work to spread best business practices across ESD managed programs.

These collective approaches to strengthen technology management across ESD will improve performance, reduce inefficiency and duplication, and provide the support needed to achieve our Mission.

ESD Division Chiefs, Branch Chiefs and employees will use this Information Management Strategic Plan to guide their requests for the IT ESD employs in executing its mission. I trust that this strategic plan will help you and ESD to be the catalysts for change, to improve our capabilities to prepare for and react to the unknowns we will face tomorrow, and to prepare the way for those who will follow in our footsteps to successfully carry on the ESD missions and traditions.


Craig H. Glassner
Director, Executive Services

Executive Summary

Information Technology is intertwined with the core competencies and major functions that define Executive Service Directorate's (ESD) mission. Technology and Information Management (IM) processes enable our decision making, our command and control, and our mission execution. Recognition of this convergence and our dependence on IT necessitates a planning process to effectively procure, develop, use, and secure our IM/IT systems. This IM/IT Strategic Plan lays out the way ahead for the management of IT in the directorate.

The Assistant Director for Systems and Services will update the IM/IT Strategic Plan bi-annually and provide goals, priorities, tenets, and an overview of the current strategic planning framework. In this initial plan, the emphasis is on describing a framework for IT decision-making and governance. Future updates will incorporate more specific IM/IT goals relating to our core competencies and functions.

In the past, IT decision-making was primarily decentralized to the organization level due to the way budgets were managed. As a result, DoD and WHS developed many different systems that do similar things that now have to be maintained. There is little assurance of standardization in development, information security, or compliance with the WHS enterprise network architecture. Lack of visibility at the ESD leadership level over IT-related decisions and inconsistent funding impacts our readiness and puts our mission accomplishment at risk. We must incorporate decisions on technology-enabled and technology-dependent systems and processes into our strategic planning process. Information Technology is no longer a pick-up game. The network readiness aspect, driven by the constantly increasing threat to DoD, and ESD functional information, drives the need for more consistent and centralized decision-making around our valuable IT assets.

Public law and regulatory guidance from the federal, DoD and WHS levels, necessitate changes in our IT processes so that IM/IT is treated as an investment and is managed in a way that ensures public funds are being spent wisely. Tangible return for the IM/IT investment, as measured against improvements in mission and/or program performance, is expected.

This inaugural Information Management Strategic Plan (IMSP) sets the stage for a new way of managing IM/IT in the directorate. The plan identifies IT tenets which are foundational to the use of IT to support ESD missions and explains the concept of full cycle governance and its relation to the core IM/IT processes of Policy, Enterprise Architecture, Capital Planning and Investment Management, and Modernization. Finally, the IMSP identifies goals for realization in the immediate future (FY08/09), the near (FY10-11) and the long term (FY 2012).

Section I—Introduction

1-1. Purpose.

Planning for the effective and efficient use of IT within ESD is an ongoing activity and a directorate-wide responsibility. This strategy is a guide for ESD division chiefs and branch and section managers to make informed decisions on their own IM/IT investment strategies, while ensuring consistency in IM/IT decision-making across the directorate.

1-2. Scope.

The FY 08 IMSP focuses on identification of best business practices and establishing a governance structure and framework for making decisions and investments of our IM/IT assets. Specific implementation guidance of the strategies outlined here will be captured in divisional implementation plans.

1-3. Applicability.

The IMSP applies to all divisions within ESD.

1-4. Plan Organization.

The IMSP consists of four major sections:

- Section I - Introduction
- Section II - ESD Vision, Intent, Tenets
- Section III - Strategies
- Section IV - Goals

1-5. Responsibilities

The management of information resources and IM/IT is applicable to, and the responsibility of, all ESD divisions. All IM/IT decisions involve coordination through several different organizational levels — Division level, Assistant Director level, Director level, then coordination and execution in concert with the Information Technology Directorate of WHS. Coordination will be made with OSD-CIO for enterprise-wide applications on the OSD backbone.

a. ESD Divisions will:

(1) Appoint an IM/IT point of contact to advise the Division Chief on leveraging the benefit of IT towards mission priorities.

(2) IM/IT POC will Identify requirements and programs for mission support. Coordinate and supervise the execution of IM/IT services with the Assistant Director for Systems and Services.

(3) Participate in ESD IM/IT governance as a functional lead in their particular area of expertise to advocate their needs and facilitate the transparency and effectiveness of directorate-wide IT decision-making.

(4) Provide information as needed to populate a division IM/IT implementation plan maintained by the Assistant Director for Systems and Services.

b. Assistant Director for Systems and Services:

(1) Executes the fiduciary responsibility of a CIO for ESD, inherent in the Clinger-Cohen Act of 1996.

(2) Is the proponent for the IMSP and ESD IM/IT processes.

(3) Plans and Programs for all IM/IT budget requests each FY.

(4) Coordinates IM/IT support for directorate-wide requirements.

(5) Creates and maintains a division IM/IT implementation plan.

(6) Main interface with ITMD and OSD-CIO.

(7) Functional program manager for IM/IT projects in ESD's domain.

c. ESD Domain Manager, Information Technology Management Directorate, WHS (ITMD):

(1) Provides common user IT services to ESD. Common user services include network access, telephone service, defense messaging service, E-mail messaging, common application desktop support, and maintenance of web, file and print servers. Additionally, ITMD provides for the housing of mission applications servers.

(2) Executes programmed IM/IT budget for ESD IT goods and services.

(3) Assesses and enforces compliance with DoD infrastructure standards.

(4) Responsible for ESD Information Assurance posture. ESD's domain manager will maintain access to all IM/IT resources.

(5) Technical program manager for IM/IT projects in ESD's domain.

Section II—ESD Vision and IM/IT Tenets

ESD
"Reputation for Being Responsible, Reliable, Resourceful and Relevant."

2-1. Director, Executive Services Mission and Vision.

ESD provides comprehensive administrative management and graphics services to the Office of the Secretary of Defense and executes federally mandated and regulatory programs, including Freedom of Information Act, Security Review, Privacy Act, Records Management, Directives, Forms, Declassification Review, and Information Collection, on behalf of the Secretary within the Department and externally to Government agencies and the general public.

ESD's vision is to be a creative, results driven, preeminent provider of executive services and program management within the Department and throughout the Federal Government recognized for excellence.

Director's Goals

As noted in the initial ESD Strategic Plan, the directorate must continue to position itself to excel in a divergent environment by anticipating challenges, predicting requirements, and managing change with appropriate communication and resources. Our goals continue to be:

Leadership and Communication: Responsive and reliable action is the hallmark of how ESD does business.

Superior Customer Service: ESD intensely focuses on customer needs - stated and implied, current and future.

Quality Workforce: Above all, ESD remains committed to our military members, civilians, contractors and families. We will remain directly involved in ensuring their well-being. Our people are the bedrock upon which ESD is built. Our behavior will support personal and professional growth and demonstrate mutual respect and trust. Without them, the best technology in the world is all for naught.

Stewardship and Performance Management: ESD acts ethically and measures performance through results and maximum value for taxpayer dollars.

Future Focus: The ESD strategic edge is concurrent focus on exemplary day-to-day service while positioning for the future within a changing environment. ESD strives for a common IT platform to task, track and coordinate/collaborate executive correspondence, FOIA requests, security review requests, and directives.

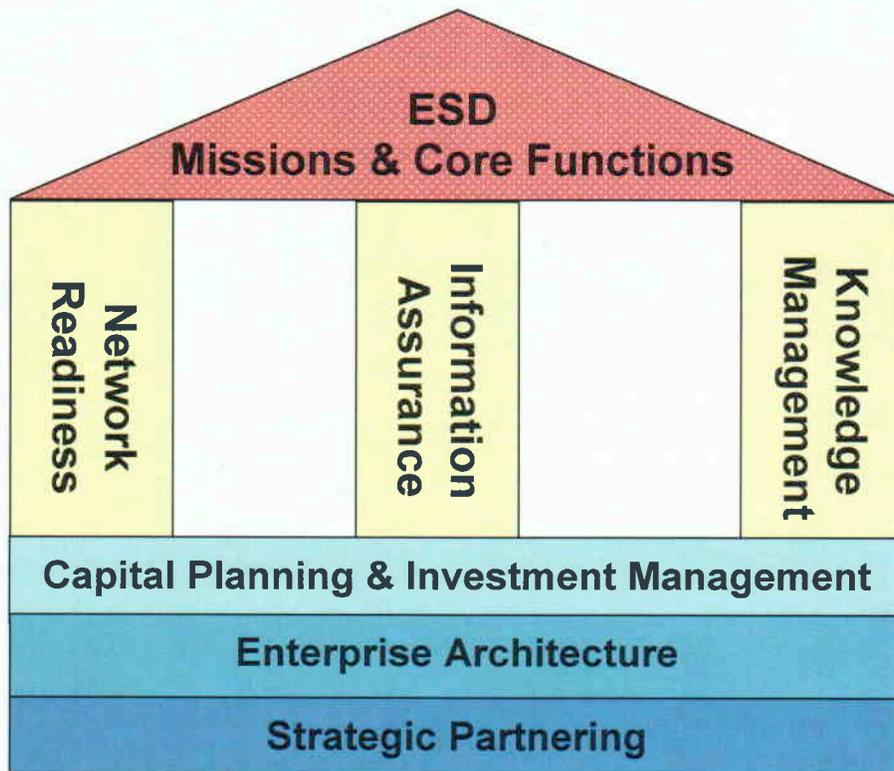
Figure 2.1 Director's goals

2-2. ESD IM/IT Vision.

ESD missions will be powered by IM/IT solutions that are integrated, secure, sustainable, scaleable, consistent with DoD enterprise standards and architecture; that embed knowledge processes to access and synchronize information; with measurable Return on Value that shows improvement to ESD operations.

Information Technology is a key enabler of accomplishing ESD missions, core functions, and the Director's goals and priorities. Decisions on the value of IT investments must reflect that investment's contribution to achieving the stated directorate priorities. When appropriate, solutions will be optimized at the enterprise level to ensure consistency, scalability, and access for all users.

2-3. IM/IT Tenets. There are six tenets that are foundational to IM/IT employment in ESD.



IM/IT TENETS

- **Network Readiness:** Information systems and IM processes will be integrated, secure, sustainable, scaleable, and compliant with DoD standards and technical requirements and the WHS enterprise architecture. Network readiness drives both our IT infostructure modernization plans and the emphasis on standardization across the directorate and the WHS enterprise.

- **Information Assurance:** Secure networks and valuable ESD information by incorporating security requirements into systems and processes during development. It is a leadership responsibility to maintain situational awareness of the continuing cyber threat and mitigating actions. Users will execute supporting policies and procedures designed to protect our information assets.

- **Knowledge Management:** Incorporate the strategies--including the optimal mix of people skills, process reengineering and technical initiatives--that promote improved capabilities and competencies for searching and sharing of accurate and relevant information. Set the conditions for a "culture of collaboration" to enable improved decision-making, leader development and increased potential for innovation.

- **Information Management/Information Technology Capital Planning and Portfolio Management:** Investment in IM/IT must support the directorate's operational priorities and have a measurable operational impact, a supportable business case, and a positive return on investment/value. Information Management/IT-based mission systems will be managed through a Portfolio Management process directed by DoD and executed by ITMD.

- **Enterprise Architecture:** Support standardization and the integration of information systems across functional areas allows the directorate to identify short-falls, and guides future priorities and POM requirements.

- **Strategic Partnering:** Every IT-enabled process or initiative is a result of a partnership between the functional/mission owner and the IM/IT provider. The functional/mission owner identifies the requirements and capabilities needed for mission accomplishment and the IM/IT provider identifies how to best achieve that mission within the supportable architecture. Additionally, cultivating strategic information exchange opportunities with industry, federal and other Department of Defense organizations provides the collaboration and exploration necessary to sustain ESD at the forward edge of technical competency and capabilities.

Figure 2.2 ESD IM/IT Tenets

2-4. IM/IT Decision Principles.

The following three principles, information assurance, enterprise solutions, and accessibility, reflect the directorate's priority for security, standardization, and efficient use of resources, and will drive IT decisions at all levels. Deviations will only be considered after analysis of operational impact and submission of a supportable business case.

a. Information Assurance: Security is the highest priority. Only acquire information systems that meet the approved DoD security features (*security*).

b. Enterprise Solutions:

(1) When applicable, capabilities will be optimized for the directorate vice the division level. Requirements common to multiple divisions are best supported with a common enterprise solution and a consolidated execution plan (*standardization, efficiency*).

(2) Standard solutions for similar requirements are preferred over equal or slightly more capable unique solutions (*standardization, efficiency, security*).

(3) ESD relies on the ITMD for infrastructure support and favors solutions that are part of the WHS standard catalogue of available service support (*standardization, efficiency*).

(4) ESD, in concert with ITMD, will leverage enterprise software agreements, plus hardware and services contracts that are already pre-competed, as its first source for IT acquisitions for workplace and appropriate mission systems. Use of standard Commercial Off-the-Shelf (COTS) products is preferred, when appropriate (*standardization, efficiency*).

c. Accessibility:

(1) Functional proponents will identify the information exchange requirements and incorporate the appropriate interfaces into the design, development, and deployment of their systems whether based on COTS or custom development. We will not perpetuate stand-alone or non-integrated systems unless there is a compelling reason to do so. (*efficiency*).

(2) Systems will be designed to pull required data from an Authoritative Data Source as identified in the DoD IT registry for data elements located on the DISA portal, <http://diides.ncr.disa.mil/mdregHomePage/mdregHome.portal>. This supports the stated DoD goals of reuse and "shareability" (*standardization, efficiency*).

(3) The domain manager will ensure that data and repositories in ESD will be indexed, meta-tagged, and accessible by authorized users. Active management of the data and content is required by the functional proponent. The data creator must

designate level of accessibility, i.e., public/general accessibility or limited use to only those who have demonstrated a need (*standardization, efficiency, security*).

Section III- Governance Strategies

3-1. Full Cycle Governance (Figure 3.1).

Planning for the effective and efficient use of IT within ESD is not a “govern-once” activity that happens at the end of the fiscal year. Full cycle governance is an overall deliberate planning process that links sound IM/IT investments to enhanced mission planning and execution. The operational decision-making process that supports governance is intricately linked to the IM/IT processes that support the execution of the IT enablement of our mission priorities. Governance provides visibility of IT spending and maintains focus on those activities that will have the most strategic value to the directorate. Information Management/IT governance is an ongoing process of selecting, controlling, and evaluating solutions and starts with the identification of a functional need or requirement that can be enabled by use of IT.

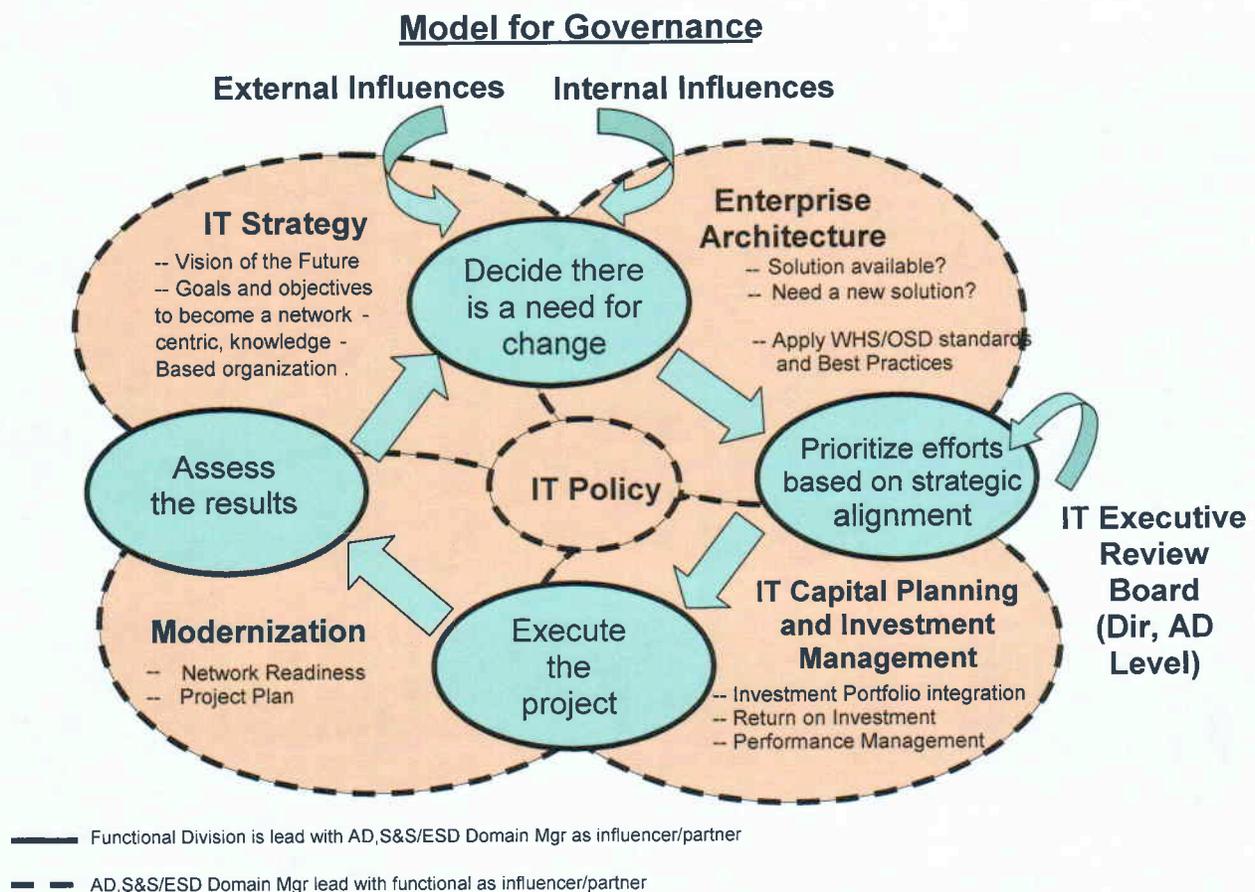


Figure 3.1 Full Cycle Governance

As shown in the Full Cycle Governance Model, each requirement is assessed against other priorities supporting core functions and evaluated against the rest of the IT portfolio in the applicable mission area. Solutions are validated against the enterprise architecture standards and driven by technical feasibility, affordability, risk management, and anticipated performance enhancements. Once accepted, the solution influences the modernization plan as it forces an addition to the architecture, but also may require modernization in other areas of the infrastructure to achieve it. Program managers and functional proponents are accountable to the leadership for successful project implementation and measurable process improvement to validate the success of the IT initiative. The effectiveness of project execution, as well as other internal and external factors, drives the ongoing assessment of whether this is the best IT strategy to meet the directorate's needs.

a. Current State: Prior to the initiative to implement a governance process, focus was almost exclusively on the execution of budgeted and year-end dollars to buy IT hardware/software/support. With the exception of directing which UFRs to fund, ESD had little control or visibility on what value was gained from those IT investments.

b. Objective State: The governance process is built upon IT requirements business cases and subject to review by senior decision-makers for certain thresholds of IT investment. Information Technology requirements are evaluated against information assurance, enterprise architecture, and affordability/value targets, as well as operational impact and strategic alignment, to ensure effective investment. During FY 08, the directorate will institute a process to capture and vet all divisional IM/IT requirements.

3-2. ESD IM/IT Governance Components.

There are five IM/IT components that support the governance process: IT Policy and Guidance, the IM Strategic Plan, Modernization Planning, Capital Planning and Investment Management, and Enterprise Architecture. (Figure 3.1)

a. Information Technology Policy and Guidance. Information Management/IT guidance and policy assist the functional user through the IT life cycle requirements development, planning, solution decision, acquisition, project implementation, performance management, sustainment, and modernization. The investment in and performance of IT has come under increasing scrutiny from the federal and legislative levels of government over the last decade. Any IM/IT decision at the local level is subject to policy requirements directed by regulatory legislation, the Office of Management and Budget, DoD, as well as local WHS policies.

Current State: We are relying on federal and DoD IM/IT policies to execute our missions. ITMD issues IA policy memos but so far has not produced any other usable policy documents.

Objective State: WHS IM/IT Policy reflects accurate procedures to effectively execute full cycle governance.

b. Enterprise Architecture. The enterprise architecture (EA) provides a blueprint for how WHS executes its mission--documenting the processes for how core functions are accomplished, the systems that support those processes and the technical standards. The EA contains both the current baseline 'As-Is' state and target 'To-Be' state. The EA provides standardization of decisionmaking related to capability delivery, however it is constantly evolving based on emerging operational requirements and technology advances. WHS follows the DoD Architecture Framework depicting an operational, systems, and technical view. The value of the EA to the local IT decision-maker is to define the business, application, infrastructure and information configurations that are currently in place. Reuse of and integration into existing standards is a more effective and efficient way to design solutions to support a network-centric, knowledge-based operation.

Current State: To date, the WHS EA identifies a partial infrastructure, application, and business architecture. The hardware and software components of workplace and training functions are managed via the WHS CIO Architecture Repository and the major business processes and systems supporting several of ESD's core functions have been identified.

Objective State: Over the next two years, ESD will work with ITMD towards a full EA. The EA provides standards for capabilities, systems, and technical specifications. The EA guides the transition to multi-functional end-to-end business processes.

c. ESD Modernization. The ESD FY Obligation Plan incorporates approved IT initiatives and network readiness considerations. It lays out the rate of modernization in manageable increments to accommodate mission priorities, level of effort and risk, and funding streams. It serves as the guideline for the annual execution plan for upgrading and maintaining IT in ESD. Network readiness is the ability of a system to meet current enterprise standards for operation and may involve hardware replacement, software upgrades, improved security configurations, or infrastructure improvements.

Current State: Ongoing modernization initiatives include a life cycle replacement of aged NIPR and SIPR workstations, peripherals (scanners, printers, software) and a common desktop configuration. ESD workplace systems use the Microsoft Enterprise License Agreement (MS ELA) instead of separate acquisitions for common productivity tools. Mission-specific requirements for Microsoft products are also supported via the MS ELA.

Objective State: All ESD Windows-based computers must run the MS XP Professional operating system by 1 October 2008 to remain compliant with DoD enterprise infostructure standards. WHS will design an operational Service Oriented Architecture that supports the centralization of hosted IT-based services such as "team room" collaboration (SharePoint Portal), learning content management system (Blackboard), and video-streaming. Transparency of IT assets provides timely visibility of network readiness needs, i.e., necessary upgrades to comply with enterprise

standards, as well as the timely replacement of equipment consistent with industry maintenance rate/failure analysis.

d. Capital Planning and Investment Management (CPIM). The CPIM lays out the strategy for ongoing identification, selection, control and evaluation of investments in information resources. The process is linked to budget formulation and focuses on ESD missions and achieving specific program outcomes. The CPIM includes IT Portfolio Management which is an inventory of functionally related technology projects and/or products reviewed for integration and synchronization.

Current State: The CPIM process is focused on review of IT-dependent unfinanced requirements (UFR) submitted to WHS FMD, as well as prioritization of IT modernization requirements submitted to WHS ITMD. The web-based ProSight system, hosted and maintained by FMD, is the definitive source for funding and prioritization decisions for lifecycle replacement and network modernization. The Assistant Director, Systems and Services is a member of the Resource Board and the Director, ESD is a member of the Senior Resource Council and provides recommendations for funding on every IT-related request based on the proposed technical solution.

Objective State: Improvement to CPIM will result from implementation of a WHS governance and IT requirements review process. The AD, S&S and the IM/IT community will become partners with the functional proponent in the requirements development, acquisition and implementation process heretofore largely the purview of the functional requirements generator. The mission systems supporting ESD functions will be managed via portfolios based on functional domains.

e. IM/IT Strategy. The strategy lays out the high-level goals and objectives for how the directorate will use IT. The strategy generally focuses on a 5-year window and is updated bi-annually to reflect changing priorities and progress.

Current State: This document is the first IM/IT strategy and primarily focuses on FYs 08/09. It is designed to lay the foundation for upcoming changes in the management of IT in ESD.

Objective State: The IM/IT Strategy will be updated bi-annually and will include directorate-wide objectives in ESD's competency areas over the next five years.

Section IV- Goals

4-1. Two years Out--FY 08-09 Goals.

With the focus on the operations in Iraq and Afghanistan, the Department has imposed severe fiscal constraints that force us to reconsider investment in IT modernization and new initiatives. This drives the directorate to make tough decisions on what technologies we will pursue for the greatest return on investment. Additionally, planning for BRAC execution will necessitate reviews of how to improve our operations through the smart use of leading technologies.

During this period the Directorate will:

- Initiate a new review process established by the Assistant Director for Systems and Services, in coordination with the ESD Domain Manager for all IT requirements and spending.
- Capture the hardware and software requirements to support productivity in the workplace and digital training environment.
- In FY 08, establish the executive governance structure, led by the Director, which ties into the Resource Council process, to make determinations on IT spending.
- Identify best IT-enabled business practices to improve productivity.
- Leverage available no and low cost assets, such as Defense Knowledge On-Line and the Microsoft operating environment procured under the WHS Enterprise License Agreement (such as Sharepoint), to infuse our business processes with knowledge-based qualities, to provide improved access to information and collaboration.
- Improve situational awareness of the cyber threat to increase responsiveness to Information Assurance policies and procedures.
- Confirm accreditation status of all systems that support ESD mission processes and develop mitigation plans for systems not in compliance.

During this period:

Information Management Division (IMD) will:

- Continue collaborating in the Federal Docket Management System Working Group to contribute to e-government initiatives and to ensure the Department interests are incorporated in system changes.
- Continue converting the inventory of current DoD forms into fillable and savable forms.
- Develop capability to integrate our business process forms with our databases to improve workflow process by electronic submission and electronic signature coordination to our databases.

Directives Division (DD) will:

- Continue refining the SD 106 process to update issuances within the Department with the use of web-based portal technology for collaboration.

Records Management and Declassification Division (RMDD) will:

- Continue the process of collecting and digitally archiving records of significance within the OSD Components.
- Investigate ways to exploit technology to improve the digital searching of record archives in response to record searches from the public and Congressional inquiry.
- Collaborate with the OSD/WHS IT community to design and implement an electronic email records management system for OSD.

Freedom of Information Division (FOID) will:

- Examine the FOIA case processing process to determine how technology would improve cycle time in closing requests.
- Reduce the present number of information systems and convert the existing data into useful management information.
- Determine technology requirements to comply with the new FOIA Executive Order and Congressional legislation.
- Explore the use of web-based portal technology to enable the public to submit and find out status of FOIA requests.

Security Review Division (SRD) will:

- Migrate security review data from the legacy Oracle database to the newly developed "Stanford" security review application.
- Continue to fine-tune requirements to the Stanford application via a configuration control process.
- Establish and maintain a security review web site. Enhance workflow process by adding web link to DefenseLink to facilitate DoD customers finding our web page and office location.
- Research and procure a software filter to remove undesired metadata that becomes attached to security review documents when they are shared in electronic format that we do not want to share with our customers.

Correspondence Control Division (CCD) will:

- Continue efforts to articulate requirements and assist in the development of the Staff Action Control and Coordination Portal (SACCP).

- Continue business process improvement efforts underway to improve management reporting in the legacy Correspondence Control System until such time that it can be replaced by SACCP.
- Provide full visibility of accountable mail, classified documents, and packages addressed to OSD.
- Examine processes within the Defense Post Office to determine if technological enhancements would improve mail handling and distribution.

Executive Support Office (ESO) will:

- Continue efforts to articulate requirements and assist in the development of the Staff Action Control and Coordination Portal (SACCP).
- Continue business process improvement efforts underway to improve management reporting in the legacy Correspondence Control System until such time that it can be replaced by SACCP.

Graphics and Presentations Division (GPD) will:

- Continue to exploit the latest graphic design technology to provide world class products and services to our customers.

4-2. Three Years Out--FY 10 Goal.

By FY 10, ESD will have a blueprint of IT assets and business processes and a set of governance principles that drives an informed discussion about the mission strategy and how it can be best supported through IT. The EA will be the basis for decision making relating to our IT assets. ESD divisions will have identified core processes that support ESD functions and the best applications/ systems to support them and work to eliminate duplicative capabilities. ESD will have a systems and technical architecture that supports a service oriented operating environment. ESD will have a high-level view of all the major business processes and systems that functional/mission leaders can use to evaluate information interface requirements and standards for systems deployment. Each IT investment will be evaluated against the vision objectives: integrated, secure, sustainable, scaleable, and knowledge-based.

4-3. Five years Out--FY 2012.

By 2012, ESD will use the EA, IM/IT capital planning and portfolio management, and a robust governance process to make every IT-related decision affecting the execution of ESD missions and core functions. Architecture-based governance will balance the need for WHAT must be done against HOW it should best be delivered to keep it consistent with DoD standards.

Summary

This strategy will set ESD in the right direction to more effectively secure our network and improve standardization, integration, and management of ESD's technology resources. Implementation of this IMSP provides an effective foundation for addressing more mission and function focused objectives in the next version. As noted in the full-cycle governance model, strategy will be periodically assessed and adjusted to fit changing requirements. With the continued support of division and branch chiefs and information managers at all levels, this strategic plan will greatly improve IM/IT management and transparency throughout the directorate and assure the core functions and Director's priorities are effectively supported with IT.

Appendix A

Definitions

Business case - A structured proposal for business improvement that functions as a decision package for organizational decisionmakers. A business case includes an analysis of business process performance and associated needs or problems, proposed alternative solutions, assumptions, constraints, and a risk-adjusted, cost-benefit analysis. [GAO]

Capital Planning and Investment Management - The CPIM process is to develop C4/IT investment policy and strategic direction that informs Army leaders and directly impacts their POM decisions on all C4/IT expenditures across all functional domains. The CPIM process is collaborative among C4/IT stakeholders, with a focus on C4/IT across the Army (to include all functional domains) throughout the life cycle of IT expenditures and the management of IT assets. [AR 25-1]

Chief Information Officer - Responsible for technology management processes that involve strategic planning, business process analysis and improvement, assessment of proposed systems, resource management (to include investment strategy), performance measurements, acquisition, and training. [AR 25-1 and Clinger-Cohen Act of 1996]

Enterprise Architecture - The explicit description of the current and desired relationships among business and management processes and IT. An enterprise architecture describes the "target" situation that the agency wishes to create and maintain by managing its IT portfolio. [AR 25-1]

Governance - The process through which organizations make strategic decisions, determine whom they involve, and demonstrate accountability for the results of their actions. The process of governance relies on a system or framework - to include Federal statutes; DoD and WHS directives, policies or guidelines; steering committees or groups; and performance measures - to define how the process is supposed to function in a particular setting. Cultural traditions, accepted practices, and codes of conduct are also instrumental in influencing the governance process. Ideally, the governance process achieves agreement between differing interests to reach a broad consensus on what is in the best interest of the enterprise.
[<http://www.army.mil/aeioo/rc/glossary.htm>]

Information Assurance (IA) - The protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. This regulation designates IA as the security discipline that encompasses Communications Security, Information Security, and control of compromising emanations (TEMPEST). [AR 25-2]

Information Management (IM) - Planning, budgeting, manipulating, and controlling of information throughout its life cycle. [AR 25-1]

Information Technology (IT) - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used directly or is used by a contractor under a contract with the executive agency which 1) requires the use of such equipment, or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (Ref. Clinger-Cohen Act of 1996.) [AR 25-1]

Infostructure - The shared computers, ancillary equipment, software, firmware and similar procedures, services, people, business processes, facilities (to include building infrastructure elements) and related resources used in the acquisition, storage, manipulation, protection, management, movement, control, display, switching, interchange, transmission, or reception of data or information in any format including audio, video, imagery, or data, whether supporting IT or National Security Systems as defined in the Clinger-Cohen Act of 1996. [AR 25-1]

IT investment portfolio - A collection of IT investments that represents the best balance of costs, benefits, and risks and is designed to improve the overall organizational performance and maximize mission performance. [AR 25-1]

IT management process - An end-to-end integrated process that includes the IM/IT business planning, business/functional process improvement, capital investment. [AR 25-1]

Network-centric, Knowledge Based force - DoD Knowledge Management (DKM) is the DoD Strategy to transform itself into a network-centric, knowledge-based force [DKM Guidance Memorandum Number 1] and the concept is incorporated into DoD IT Doctrine. Everything we do is enabled by the network and the information necessary to make decisions/take action must be relevant, accurate, and readily accessible to WHS and/or DoD Enterprise. All ESD processes and systems must be designed to take advantage of the accessibility the network offers, as well as protect the information from those not authorized to have it. Knowledge-based processes are user/decision-maker-focused either pushing relevant, targeted information to you or allowing query, search, and pull of accurate data from authoritative sources, creation/update of information based on changing reality and making it accessible to others who might need it for their decision-making.

Performance management - The use of performance measurement information to help set agreed-upon performance goals, allocate and prioritize resources, inform managers to either confirm or change current policy or program directions to meet those goals, and report on the success in meeting those goals. [AR 25-1]

Performance measure - A quantitative or qualitative characterization of performance. [AR 25-1]

Performance measurement - A process of accessing progress toward achieving predetermined goals, including information on the efficiency with which resources are transformed into goods and services (outputs), the quality of those outputs (how well they are delivered to clients and the extent they are satisfied), and outcomes (the results of a program activity compared to its specific contributions to program objectives. [AR 25-1]

Service Oriented Architecture - An architecture built around a collection of reusable components with well-defined interfaces. [CIO Magazine, Jan 15, 2004; <http://www.cio.com/archive/011504/soa.html>.] A service-oriented architecture is essentially a collection of services. These services communicate with each other...can involve either simple data passing or it could involve two or more services coordinating some activity. Some means of connecting services to each other is needed. [<http://www.service-architecture.com/>; 23 June 05.]

Appendix B

Regulatory Guidance and Related Publications

Clinger Cohen Act of 1996 (Public Law 104-106) - Establishes the position of CIO in executive agencies. The CIO management focuses on those policies, processes, and organizational responsibilities necessary to accomplish the information resources management missions defined as primary in governing legislation and other guidance. Such responsibilities include strategic planning, business process analysis and improvement, IT architecture, resource management (to include capital planning and investment strategy), performance measurements, IT acquisition, and IT workforce.

Federal Information Security Management Act of 2002 - Mandates that the security status of DoD information systems be documented, updated, and verified at least annually. The DoD Information Technology Registry is used to implement this requirement.

Government Performance and Results Act (GPRA) - Signed into law in 1993, the GPRA requires federally funded agencies to develop and implement an accountability system based on performance measurement, including the establishment of strategic plans, performance plans, and performance reports. The law emphasizes what is being accomplished, as opposed to what is being spent.

OMB Cir A-130 - Management of Federal Information Resources.

Administrative Instruction 56 - Automated Information Resource Management (AIRM) in the Office of the Secretary of Defense (OSD) and the Washington Headquarters Services (WHS), 10 Aug 1991.

DOD Dir 8000.01 - DoD Information Resources Management Program, 27 Feb 2002.

DOD Dir 8115.01 - Information Technology Portfolio Management, 10 Oct 2005.

Army Regulation (AR) 25-1 - Army Knowledge Management and Information Technology Management, June 2004.

Army Regulation (AR) 25-2 - Information Assurance, November 2003.