Software-Related Issues – Core Competencies, Legislation, Policy, etc.

Robert Gold
OUSD(AT&L)DS/SIS
703-602-0851 x103
rob.gold@osd.mil

March 13, 2003

DoD Core Competencies

- Tell us what acquisition skills Government can improve
  - Identify those critical skills only we can do
  - Identify those skills we think we need but actually impede progress
- Critical fields
  - Systems Engineers
  - Software Acquisition
  - IT

Systems Engineering

- Policy
- Architecture And Interoperability
- Systems Analysis And Control Tools
- Integrated Product & Process Development
- Technology Management
- DoD Software Acquisition Planning And Strategy
- DoD Software Acquisition Control And Methodology
- Dod Software Acquisition Planning And Strategy
- Software Management Exercise (Case Scenario And Workshop)
- Concept And Technology Development
- Environment, Safety & Health
- Benefits And Challenges Of International Cooperation
- System Definition
- Design, Fabrication And Test
- Current Events & Issues
- Production
- Deployment, Operations And Support
- Improvements To Existing Weapon Systems
- Modeling & Simulation
- Professional Ethics

Software Acquisition

- Acquisition Strategies
- Architecture
- Contracting Issues
- Configuration Management
- Cost & Schedule Estimation
- Program/Project office organization & relationships
- Software developing and acquiring maturity
- Engineering Approaches & Methodologies
- Technical Assessments
- Interoperability
- SW Verification and Validation
- Lifecycle Management
- Metrics
- Open Systems
- Software Quality Management
- Software Requirements Management
- Software reviews and audits
- Software reuse
- Risk Management
- Software Security
- Software testing issues
- Emerging issues & technologies

IT Career Field

- Policies, Laws, Regulations
- IT-related Project/Program Management
- IT Enterprise Architecture
- IT Acquisition Strategies
- Best Business Practices
- IT-related Performance Measures and Quality Management
- Capital Planning and Investment Control (CPIC)
- Acquisition Planning, Solicitation and Administration
- IT Systems Engineering
- Information Assurance
- IT-Related Technologies
- System Test and Evaluation and Software Verification and Validation

Legislation

- 2003 Auth Act Sections
  - 803 Sets guidelines and limitations on applying Spiral Development
  - 804 Requires Services and MDAP Agencies establish software acquisition improvement programs
- 2001 Auth Act Section 811
  - Requires registration with DoD Chief Information Officer
- Government Information Security Reform Act (P.L. 106-398 Subtitle G)
  - Requires annual IA eval and report
  - Renewed for DoD in 2003 Authorization Act
- Clinger Cohen Act (40 U.S.C.1452)
  - General requirements and organization for Federal IT
  - Includes National Security Systems
- E Gov Act (P.L. 107-347)
  - For NSS –
    - Standards and policies as required by the President or law
    - Electronic signature & Crisis management
  - For IT in general - FISMA

Do we need law to do the Right Thing?

SEC. 803. Spiral Development Under MDAPs

(a) AUTHORITY- The Secretary of Defense is authorized to conduct major defense acquisition programs as spiral development programs.

(b) LIMITATION ON SPIRAL DEVELOPMENT PROGRAMS- A research and development program for a major defense acquisition program of a military department or Defense Agency may not be conducted as a spiral development program unless the Secretary of Defense approves the spiral development plan for that research and development program in accordance with subsection (c). The Secretary of Defense may delegate authority to approve the plan to the Under Secretary of Defense for Acquisition, Technology, and Logistics, or to the senior acquisition executive of the military department or Defense Agency concerned, but such authority may not be further delegated.

(c) SPIRAL DEVELOPMENT PLANS- A spiral development plan for a research and development program for a major defense acquisition program shall, at a minimum, include the following matters:

(1) A rationale for dividing the research and development program into separate spirals, together with a preliminary identification of the spirals to be included.

(2) A program strategy, including overall cost, schedule, and performance goals for the total research and development program.

(3) Specific cost, schedule, and performance parameters, including measurable exit criteria, for the first spiral to be conducted.

(4) A testing plan to ensure that performance goals, parameters, and exit criteria are met.

(5) An appropriate limitation on the number of prototype units that may be produced under the research and development program.

(6) Specific performance parameters, including measurable exit criteria, that must be met before the major defense acquisition program proceeds into production of units in excess of the limitation on the number of prototype units.

(d) GUIDANCE- Not later than 120 days after the date of the enactment of this Act, the Secretary of Defense shall issue guidance for the implementation of spiral development programs authorized by this section. The guidance shall include appropriate processes for ensuring the independent validation of exit criteria being met, the operational assessment of fieldable prototypes, and the management of spiral development programs.

(e) REPORTING REQUIREMENT- The Secretary shall submit to Congress by September 30 of each of 2003 through 2008 a status report on each research and development program that is a spiral development program. The report shall contain information on unit costs that is similar to the information on unit costs under major defense acquisition programs that is required to be provided to Congress under chapter 144 of title 10, United States Code, except that the information on unit costs shall address projected prototype costs instead of production costs.

(f) APPLICABILITY OF EXISTING LAW- Nothing in this section shall be construed to exempt any program of the Department of Defense from the application of any provision of chapter 144 of title 10, United States Code, section 139, 181, 2366, 2399, or 2400 of such title, or any requirement under Department of Defense Directive 5000.1, Department of Defense Instruction 5000.2, or Chairman of the Joint Chiefs of Staff Instruction 3170.01B in accordance with the terms of such provision or requirement.

(g) DEFINITIONS- In this section:

(1) The term `spiral development program', with respect to a research and development program, means a program that--

(A) is conducted in discrete phases or blocks, each of which will result in the development of fieldable prototypes; and

(B) will not proceed into acquisition until specific performance parameters, including measurable exit criteria, have been met.

(2) The term `spiral' means one of the discrete phases or blocks of a spiral development program.

(3) The term `major defense acquisition program' has the meaning given such term in section 139(a)(2)(B) of title 10, United States Code.

2003 Auth Act Section 804

a) ESTABLISHMENT OF PROGRAMS-

(1) The Secretary of each military department shall establish a program to improve the software acquisition processes of that military department.

(2) The head of each Defense Agency that manages a major defense acquisition program with a substantial software component shall establish a program to improve the software acquisition processes of that Defense Agency.

(3) The programs required by this subsection shall be established not later than 120 days after the date of the enactment of this Act.

(b) PROGRAM REQUIREMENTS- A program to improve software acquisition processes under this section shall, at a minimum, include the following:

(1) A documented process for software acquisition planning, requirements development and management, project management and oversight, and risk management.

(2) Efforts to develop appropriate metrics for performance measurement and continual process improvement.

(3) A process to ensure that key program personnel have an appropriate level of experience or training in software acquisition.

(4) A process to ensure that each military department and Defense Agency implements and adheres to established processes and requirements relating to the acquisition of software.

(c) DEPARTMENT OF DEFENSE GUIDANCE- The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, in consultation with the Under Secretary of Defense for Acquisition, Technology, and Logistics, shall--

(1) prescribe uniformly applicable guidance for the administration of all of the programs established under subsection (a) and take such actions as are necessary to ensure that the military departments and Defense Agencies comply with the guidance; and

(2) assist the Secretaries of the military departments and the heads of the Defense Agencies to carry out such programs effectively by--

(A) ensuring that the criteria applicable to the selection of sources provides added emphasis on past performance of potential sources, as well as on the maturity of the software products offered by the potential sources; and

(B) identifying, and serving as a clearinghouse for information regarding, best practices in software development and acquisition in both the public and private sectors.

FY 2001 Auth Act Section 811

(B) prohibit the award of any contract for the acquisition of a mission critical or mission essential information technology system until--

(i) the system has been registered with the Chief Information Officer of the Department of Defense;

(ii) the Chief Information Officer has received all information on the system that is required under the directive to be provided to that official; and

(iii) the Chief Information Officer has determined that there is in place for the system an appropriate information assurance strategy; and

(C) require that, in the case of each system registered pursuant to subparagraph (B)(i), the information required under subparagraph (B)(ii) to be submitted as part of the registration shall be updated on not less than a quarterly basis.

(c) MILESTONE APPROVAL FOR MAJOR AUTOMATED INFORMATION SYSTEMS- The revised directive required by subsection (b) shall prohibit Milestone I approval, Milestone II approval, or Milestone III approval (or the equivalent) of a major automated information system within the Department of Defense until the Chief Information Officer has determined that--

(1) the system is being developed in accordance with the requirements of division E of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

(2) appropriate actions have been taken with respect to the system in the areas of business process reengineering, analysis of alternatives, economic analysis, and performance measures; and

(3) the system has been registered as described in subsection (b)(2)(B).

E-Gov Act P.L. 107-347

Title II – Federal Management and Promotion of Electronic Government Services

- Only Sections 203 and 214 are applicable to NSS
- Electronic signature, Enhancing crisis management

Title III – Information Security

Sec. 3547. National security systems

`The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency--

`(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

`(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

`(3) complies with the requirements of this subchapter.

Sec. 11331. Responsibilities for Federal information systems standards

NATIONAL SECURITY SYSTEMS- Standards and guidelines for national security systems (as defined under this section) shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

Sec. 3545. Annual independent evaluation

a) IN GENERAL- (1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

(c) NATIONAL SECURITY SYSTEMS- For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed--

(1) only by an entity designated by the agency head; and

(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

Questions & Discussion

Status of 5000.1 and 5000.2

- 5000.1 identifies principles under which acquisitions will be conducted
- 5000.2 documents revised acquisition process
- Latest versions completed SD106 review
  - Awaiting final (DepSecDef) signature

What makes Good Policy?

5000.1
3.16 Software Intensive Systems

- Acquisitions of software intensive systems shall use process improvement and performance measures. Selection of sources shall include consideration of product maturity and past performance.

5000.1
3.19 Total Systems Approach

- The PM shall be the single point of accountability for accomplishment of program objectives for total life-cycle systems management, including sustainment. The PM shall apply a human systems integration approach to optimize total system performance (hardware, **software**, and human), and when assessing operational effectiveness and suitability, and survivability, and affordability. Planning for Operation and Support and the estimation of total ownership costs shall begin as early as possible.

5000.1
3.15 Systems Engineering

- Acquisition programs shall be managed through the application of a systems engineering approach that optimizes total system performance and minimizes total ownership costs. **A modular, open-systems approach shall be employed**.

Questions & Discussion

5000.2 – SDD Entrance Criteria

- 3.7.2 Entrance Criteria.
  - Entrance into this phase depends on **technology maturity (including software),** validated requirements, and funding. Unless some other factor is overriding in its impact, the maturity of the technology shall determine the path to be followed. Programs that enter the acquisition process at Milestone B shall have an ICD that provides the context in which the capability was determined and validated.

5000.2 – Beyond CDR

- 3.7.4 Proceeding Beyond Critical Design Review.
  - The Critical Design Review during SDD provides an opportunity for mid-phase assessment of design maturity as evidenced by such measures as, for example, the number of completed subsystem and system design reviews successfully completed; the percentage of drawings completed; **planned corrective actions to hardware/software deficiencies**; adequate development testing; an assessment of environmental, safety and health risks; a completed failure modes and effects analysis; the identification of key system characteristics and critical manufacturing processes; and the availability of reliability targets and a growth plan; etc. Successful completion of the Critical Design Review ends System Integration and continues the SDD phase into the System Demonstration effort.

5000.2 – Production & Deployment

- 3.8.1.1 The purpose of the Production and Deployment phase is to achieve an operational capability that satisfies mission needs. Operational test and evaluation shall determine the effectiveness and suitability of the system. The MDA shall make the decision to commit the Department to production at Milestone C. **Milestone C authorizes entry into Low-Rate Initial Production (LRIP) (for MDAPs and major systems), into production or procurement (for non-major systems that do not require LRIP) or into limited deployment in support of operational testing for MAIS programs or software-intensive systems with no production components.** The tables at enclosure 3 identify the statutory and regulatory requirements that must be met at Milestone C.

5000.2 – Production & Deployment

- 3.8.2 Entrance Criteria.
  - Entrance into this phase depends on the following criteria: acceptable performance in development, test and evaluation and operational assessment; **mature software capability**; no significant manufacturing risks; manufacturing processes under control (if Milestone C is full-rate production); a validated Capability Production Document (CPD); acceptable interoperability; acceptable operational supportability; compliance with the DoD Strategic Plan; and demonstration that the system is affordable throughout the life cycle, optimally funded, and properly phased for rapid acquisition. The CPD reflects the operational requirements resulting from SDD and details the performance expected of the production system. If Milestone C approves LRIP, a subsequent review and decision shall authorize full-rate production.

5000.2 - LRIP

- 3.8.3.4 **LRIP is not applicable to AISs or software intensive systems with no developmental hardware; however, a limited deployment phase may be applicable. Software shall have demonstrated the maturity level required in the CPD prior to deploying it to the operational environment. Once the maturity level has been demonstrated, the system or increment is baselined, and a methodical and synchronized deployment plan is implemented for all applicable locations.**

5000.2 – Full-Rate Production

- 3.8.4 Full-Rate Production Criteria.
  - An MDAP may not proceed beyond LRIP without approval of the MDA. The available knowledge to support this approval shall include demonstrated control of the manufacturing process and reliability, the collection of statistical process control data, and the demonstrated control and capability of other critical processes. **The decision to continue beyond low-rate to full-rate production, or beyond limited deployment of AISs or software-intensive systems with no developmental hardware, shall require completion of IOT&E, submission of the Beyond LRIP Report for DOT&E Oversight Programs, and submission of the LFT&E Report (where applicable) to Congress, to the Secretary of Defense, and to the USD(AT&L).**

5000.2 – Software Resources Data Report

- Required for all major contracts and subcontracts, regardless of contract type, for contractors developing/producing software elements within ACAT I and ACAT IA programs for any software development element with a projected software effort greater than $25M (FY 2002 constant dollars).
- Submit data on each software element at the following times:
  - 180 days prior to contract award
  - 60 days after contract award
  - 60 days after start of subsequent software releases
  - within 120 days after software release or final delivery
- Reported data: System context, Size, Effort, Schedule and Quality

5000.2 – TAB 4

- IT Considerations
  - This section contains general policy and procedures associated with IT acquisition and MAIS.
  - Limited applicability to MDAPs and IT-intensive weapons systems depending upon interconnection to the GIG
    - CCA Confirmation
    - Mission Critical System
      - Register with the CIO
      - CIO reviews IA strategy
      - CIO confirms acquisition meets CCA requirements
    - IA Strategy
    - C4ISR Plan

5000.2 CCA Compliance Table

Requirements Related to the Clinger-Cohen Act (CCA) of 1996 (reference XX)	Applicable Program Documentation **
***Make a determination that the acquisition supports core, priority functions of the Department	ICD Approval
***Establish outcome-based performance measures linked to strategic goals	ICD, CDD, CPD and APB approval
***Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of commercial-off-the-shelf (COTS) technology	Approval of the ICD, Concept of Operations, AoA, CDD, and CPD
* No Private Sector or Government source can better support the function	Acquisition Strategy page XX, para XX AOA page XX
* An analysis of alternatives has been conducted	AOA
* An economic analysis has been conducted that includes a calculation of the return on investment; or for non-AIS programs, a Life-Cycle Cost Estimate (LCCE) has been conducted	Program LCCE Program Economic Analysis for MAIS
There are clearly established measures and accountability for program progress	Acquisition Strategy page XX APB
The acquisition is consistent with the Global Information Grid policies and architecture, to include relevant standards	APB (Interoperability KPP) C4ISP (IERS)
The program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards	Information Assurance Strategy
To the maximum extent practicable, (1) modular contracting has been used, and (2) the program is being implemented in phased, successive increments, each of which meets part of the mission need and delivers measurable benefit, independent of future increments	Acquisition Strategy page XX
The system being acquired is registered	Registration Database

5000.2 TAB 4 - ESI

- E4.2.7 When use of commercial IT is considered viable, maximum leverage of and coordination with the DoD Enterprise Software Initiative shall be made.

5000.2 – TAB 5 T&E

- E5.7.5 **Hardware and software alterations that materially change system performance, including system upgrades and changes to correct deficiencies, shall undergo OT&E.**

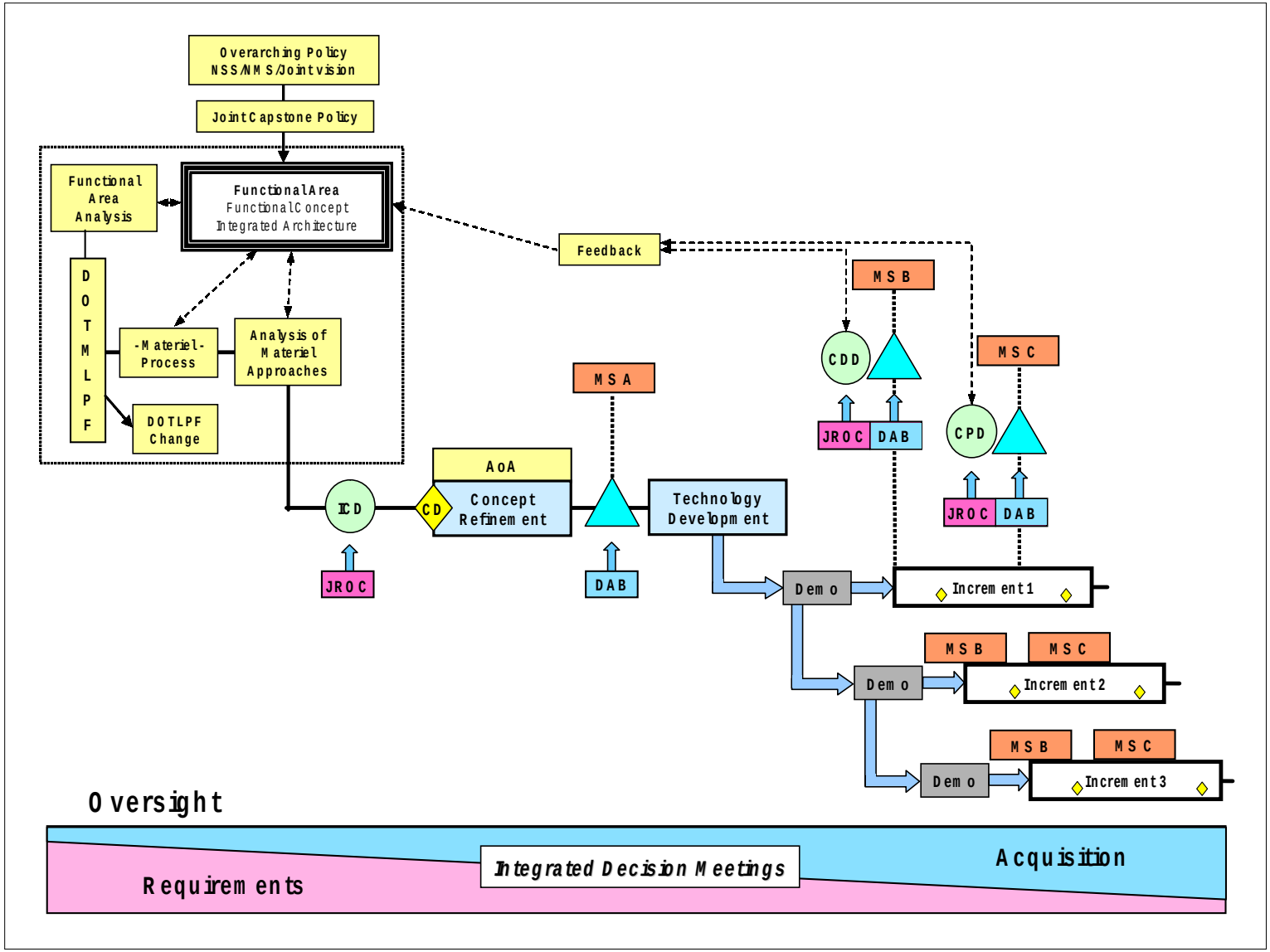
Questions & Discussion

Other DoD Policy

CJCS 3170 - Requirements Generation System

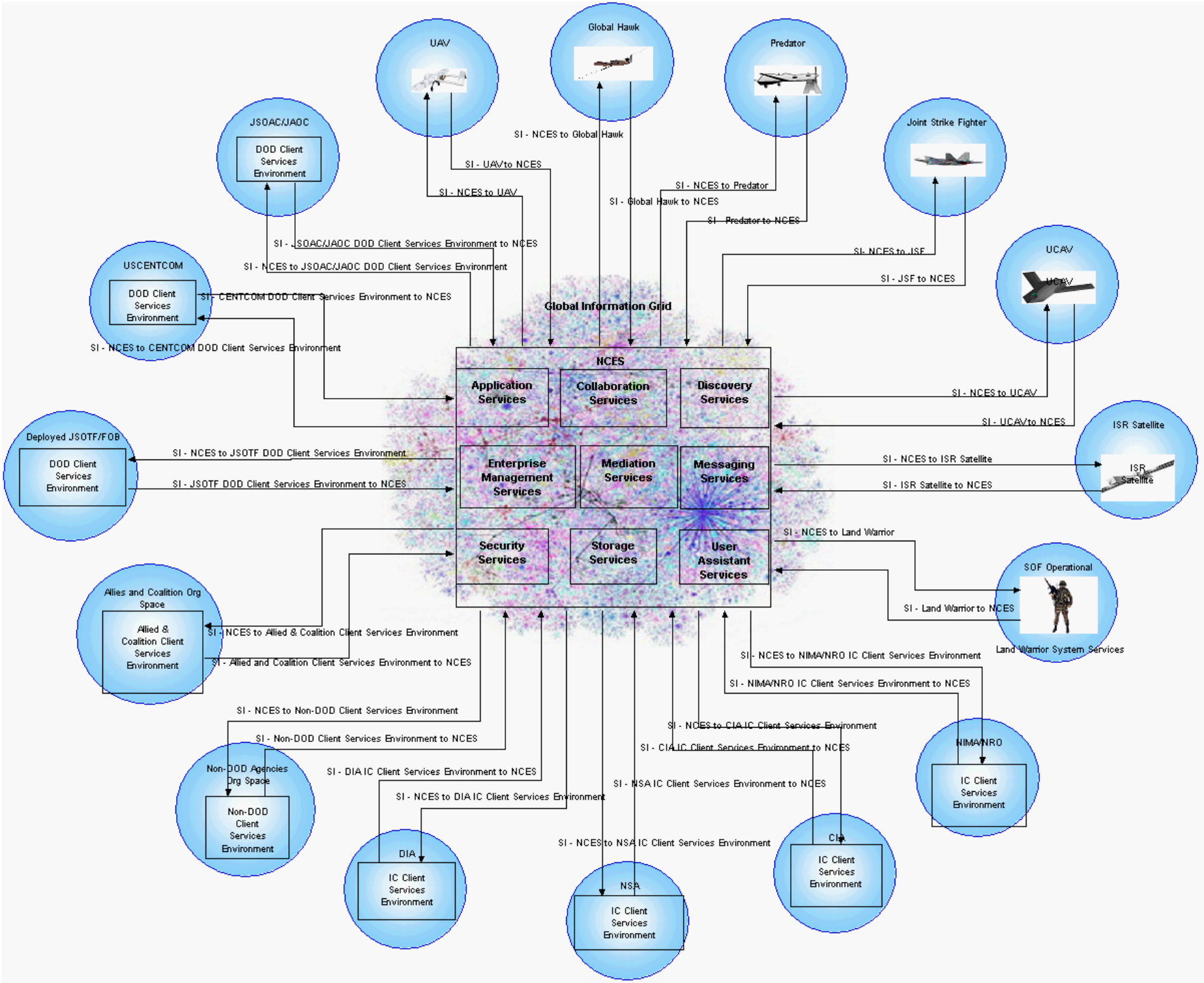
- Documents JCS requirements management process
- Partial revision changes
  - From threat-based to capabilities-based methodology
  - Top-down effort starting with joint warfighting needs
- Replaces MNS, ORD etc. with ICD, CDD etc.
- Revised 3170 not issued yet
  - DRAFT title – Joint Capabilities Integration and Development System (JCIDS)
- Revised methodology addressed in draft 5000 series

5000.2 Requirements and Acquisition Process Depiction



Global Information Grid – 8100.1

- Governs globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel.
- In practice, does not cover –
  - Equipment integral to a weapon or weapons system except where connected to the GIG
  - FMMP-governed IT (business, personnel etc.)
- Co-governs DoD intelligence systems along with equivalent CIA documents


UAV
Global Hawk
Predator
Joint Strike Fighter
UCAV
JSOAC/JAOC
DOD Client Services Environment
USCENTCOM
DOD Client Services Environment
Deployed JSOTF/FOB
DOD Client Services Environment
Allies and Coalition Org Space
Allied & Coalition Client Services Environment
Non-DOD Agencies Org Space
Non-DOD Client Services Environment
DIA
IC Client Services Environment
NSA
IC Client Services Environment
CIA
IC Client Services Environment
NIMA/NRO
IC Client Services Environment
SOF Operational
Land Warrior System Services
ISR Satellite
ISR Satellite
Global Information Grid
NCES
Application Services
Collaboration Services
Discovery Services
Enterprise Management Services
Mediation Services
Messaging Services
Security Services
Storage Services
User Assistant Services
SI - NCES to Global Hawk
SI - UAV to NCES
SI - NCES to UAV
SI - Global Hawk to NCES
SI - NCES to Predator
SI - Predator to NCES
SI - NCES to JSF
SI - JSF to NCES
SI - JSOAC/JAOC DOD Client Services Environment to NCES
SI - NCES to JSOAC/JAOC DOD Client Services Environment
SI - CENTCOM DOD Client Services Environment to NCES
SI - NCES to CENTCOM DOD Client Services Environment
SI - NCES to UCAV
SI - UCAV to NCES
SI - NCES to JSOTF DOD Client Services Environment
SI - JSOTF DOD Client Services Environment to NCES
SI - NCES to ISR Satellite
SI - ISR Satellite to NCES
SI - NCES to Land Warrior
SI - Land Warrior to NCES
SI - NCES to Allied & Coalition Client Services Environment
SI - Allied and Coalition Client Services Environment to NCES
SI - NCES to NIMA/NRO IC Client Services Environment
SI - NIMA/NRO IC Client Services Environment to NCES
SI - NCES to Non-DOD Client Services Environment
SI - Non-DOD Client Services Environment to NCES
SI - NCES to CIA IC Client Services Environment
SI - CIA IC Client Services Environment to NCES
SI - DIA IC Client Services Environment to NCES
SI - NCES to DIA IC Client Services Environment
SI - NSA IC Client Services Environment to NCES
SI - NCES to NSA IC Client Services Environment

8500.1 and 8500.2 Information Assurance

- Provides policy and procedural framework under which GIG IA will be addressed
  - Does NOT include requirements for Intelligence connectivity
- Applicable only to GIG and those portions of weapons systems that actually connect to the GIG
- May be used across a weapons system at the discretion of the PM
- Will be augmented by IA acquisition policy 8580 co-authored by AT&L and C3I

8500 Series framework

- 8500 - General
- 8510 - Certification and Accreditation
- 8520 - Security Management (SMI, PKI, KMI, EKMS)
- 8530 - Computer Network Defense/Vulnerability Mgt
- 8540 - Interconnectivity/Multi-Level Security (SABI)
- 8550 - Network/Web (Access, Content, Privileges)
- 8560 - Assessments (Red Team, TEMPEST Testing & Monitoring)
- 8570 - Education, Training, Awareness
- 8580 - Other (Mobile Code, IA OT&E, IA in Acquisition)

IT Registry

- Registry potentially satisfies several requirements
  - Interfaces/contingency plans (CCA, Sect 811 of 01 NDAA)
  - FMIT mgmt (PL 107-117 Sect 8104)
  - PKI
  - COOP/Contingency plan
  - Basis for GISRA annual report
- Guidance for this year's registry under development
  - Currently assessing registration of only those portions of weapons systems with interconnects

Wireless Devices 8100

- Addresses use of commercial wireless devices by DoD
  - Requires encryption of data on Personal Electronic Devices (including laptops)
- Currently under review by C3I and AT&L community

Biometrics

- Defined as an “automated method of authenticating or verifying an individual based upon a physical or behavioral characteristic of that individual”.
- Army is DoD focal point for biometrics.
- The draft policy requires that DoD “incorporate biometrics in all new acquisitions and upgrades of DoD owned or operated systems that receive, process, store or transmit information whenever possible”.
- Primary weapons systems concern is impact to ability to perform the mission because of unnecessary biometrics.
- Additional concerns include cost and schedule impacts to ongoing and future acquisitions.
- Policy document has not yet been signed.

Other Policy Initiatives

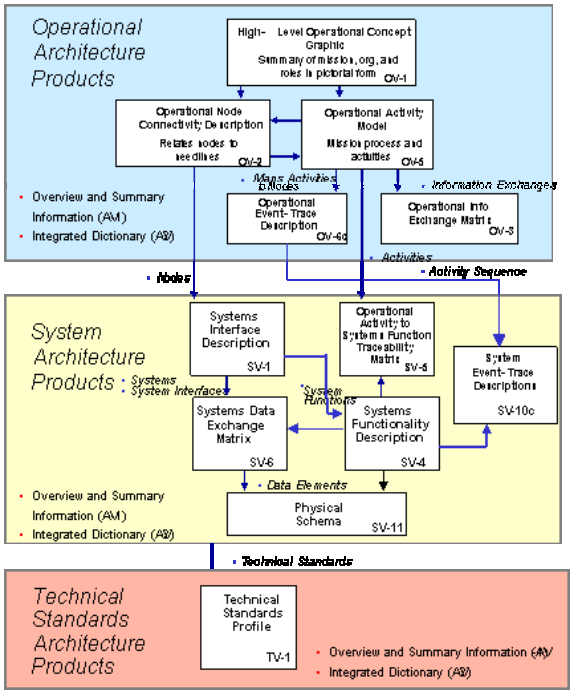
- Evolving IO (interoperability) Key Performance Parameter (KPP) to Net-ready KPP
  - Includes both Information Exchange Requirements and Information Assurance requirements for connectivity to the GIG
- Data Management and Knowledge Management
- Financial Management Modernization Program & Human Resources Systems
  - Includes financial and non-financial operations/systems
  - May impact weapons systems programs if these functions are incorporated into the weapons system acquisition
  - Based on legislation and DoD memo
- Architectures

Architectures

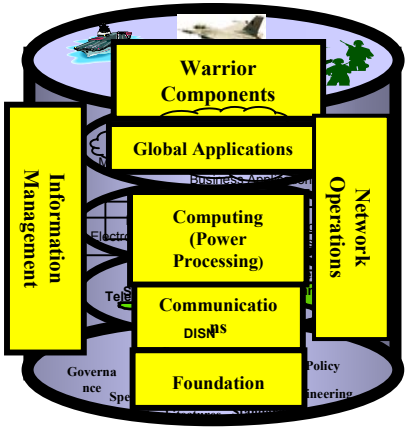
- DoD Architecture Framework
- GIG Architecture
- Financial Management Enterprise Architecture
- Federal Enterprise Architecture

DoD Architectures

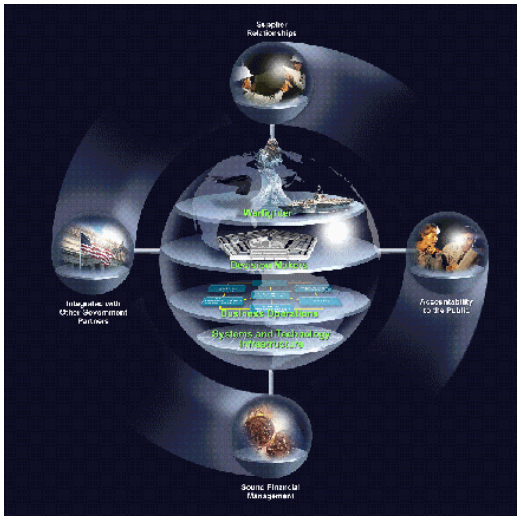
DoD Architecture Framework



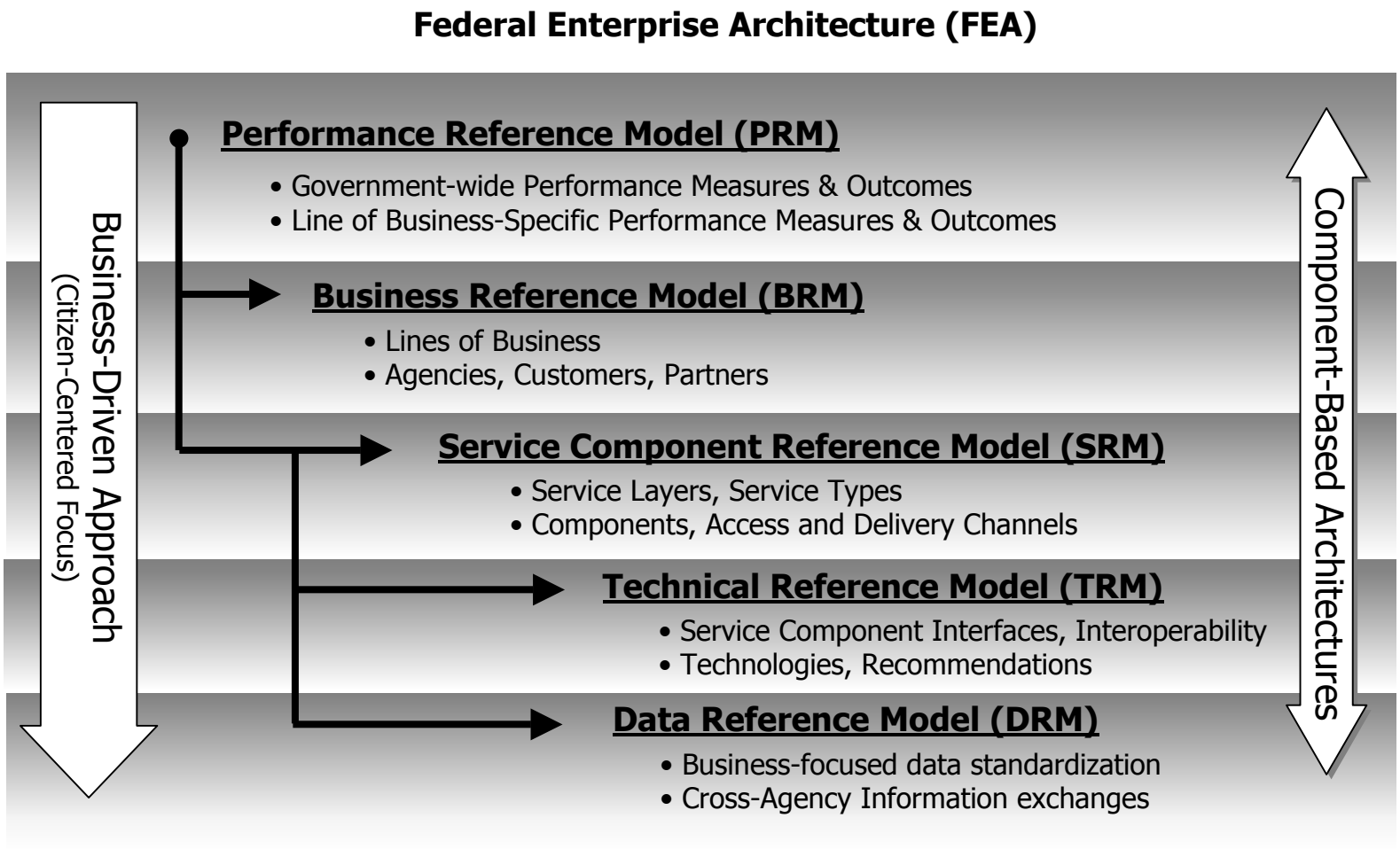
GIG Arch



Financial Mgmt Enterprise Arch



Federal Enterprise Architecture



Software from Government Supply Sources

- FAR/DFARs modified to allow contractors to purchase software from Government sources
  - FAR 52.251-1, Government Supply Sources
  - SUBPART 208.74--ENTERPRISE SOFTWARE AGREEMENTS (added 25 Oct, 2002)
  - SUBPART 251.1--CONTRACTOR USE OF GOVERNMENT SUPPLY SOURCES
  - 252.251-7000 Ordering From Government Supply Sources
- Enterprise Software Initiative (ESI)
  - http://www.don-imit.navy.mil/esi
- May be expanded to address needs of software developers
  - Compilers, CASE, real-time OS, etc.

Community of Practice

- SE CoP (www.pmcop.dau.mil) has been expanded to include software-related topics
- Two software experts will be SE CoP discussion editors
  - Software Cost Estimating – Tom McGibbon (DACS)
  - CMMI – Jim Belford (STSC)
- CoP administrators will streamline account process for Collaborators

Questions & Discussion

BACK UP SLIDES

2001 Auth Act Section 811

(a) RESPONSIBILITY OF DOD CHIEF INFORMATION OFFICER RELATING TO MISSION CRITICAL AND MISSION ESSENTIAL INFORMATION TECHNOLOGY SYSTEMS- Section 2223(a) of title 10, United States Code, is amended--

(1) by striking `and' at the end of paragraph (3);

(2) by striking the period at the end of paragraph (4) and inserting `; and'; and

(3) by adding at the end the following:

`(5) maintain a consolidated inventory of Department of Defense mission critical and mission essential information systems, identify interfaces between those systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems.'.

(b) MINIMUM PLANNING REQUIREMENTS FOR THE ACQUISITION OF INFORMATION TECHNOLOGY SYSTEMS-

(1) Not later than 60 days after the date of the enactment of this Act, Department of Defense Directive 5000.1 shall be revised to establish minimum planning requirements for the acquisition of information technology systems.

(2) The revised directive required by (1) shall--

(A) include definitions of the terms `mission critical information system' and `mission essential information system';

(B) prohibit the award of any contract for the acquisition of a mission critical or mission essential information technology system until--

(i) the system has been registered with the Chief Information Officer of the Department of Defense;

(ii) the Chief Information Officer has received all information on the system that is required under the directive to be provided to that official; and

(iii) the Chief Information Officer has determined that there is in place for the system an appropriate information assurance strategy; and

(C) require that, in the case of each system registered pursuant to subparagraph (B)(i), the information required under subparagraph (B)(ii) to be submitted as part of the registration shall be updated on not less than a quarterly basis.

(c) MILESTONE APPROVAL FOR MAJOR AUTOMATED INFORMATION SYSTEMS- The revised directive required by subsection (b) shall prohibit Milestone I approval, Milestone II approval, or Milestone III approval (or the equivalent) of a major automated information system within the Department of Defense until the Chief Information Officer has determined that--

(1) the system is being developed in accordance with the requirements of division E of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

(2) appropriate actions have been taken with respect to the system in the areas of business process reengineering, analysis of alternatives, economic analysis, and performance measures; and

(3) the system has been registered as described in subsection (b)(2)(B).

(d) NOTICE OF REDESIGNATION OF SYSTEMS-

(1) Whenever during fiscal year 2001, 2002, or 2003 the Chief Information Officer designates a system previously designated as a major automated information system to be in a designation category other than a major automated information system, the Chief Information Officer shall notify the congressional defense committees of that designation. The notice shall be provided not later than 30 days after the date of that designation. Any such notice shall include the rationale for the decision to make the designation and a description of the program management oversight that will be implemented for the system so designated.

(2) Not later than 60 days after the date of the enactment of this Act, the Chief Information Officer shall submit to the congressional defense committees a report specifying each information system of the Department of Defense previously designated as a major automated information system that is currently designated in a designation category other than a major automated information system including designation as a `special interest major technology initiative'. The report shall include for each such system the information specified in the third sentence of paragraph (1).

2001 Auth Act Section 811(cont'd)

(e) ANNUAL IMPLEMENTATION REPORT-

(1) The Secretary of Defense shall submit to the congressional defense committees, not later than April 1 of each of fiscal years 2001, 2002, and 2003, a report on the implementation of the requirements of this section during the preceding fiscal year.

(2) The report for a fiscal year under paragraph (1) shall include, at a minimum, for each major automated information system that was approved during such preceding fiscal year under Department of Defense Directive 5000.1 (as revised pursuant to subsection (b)), the following:

(A) The funding baseline.

(B) The milestone schedule.

(C) The actions that have been taken to ensure compliance with the requirements of this section and the directive.

(3) The first report shall include, in addition to the information required by paragraph (2), an explanation of the manner in which the responsible officials within the Department of Defense have addressed, or intend to address, the following acquisition issues for each major automated information system planned to be acquired after that fiscal year:

(A) Requirements definition.

(B) Presentation of a business case analysis, including an analysis of alternatives and a calculation of return on investment.

(C) Performance measurement.

(D) Test and evaluation.

(E) Interoperability.

(F) Cost, schedule, and performance baselines.

(G) Information assurance.

(H) Incremental fielding and implementation.

(I) Risk mitigation.

(J) The role of integrated product teams.

(K) Issues arising from implementation of the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Plan required by Department of Defense Directive 5000.1 and Chairman of the Joint Chiefs of Staff Instruction 3170.01.

(L) Oversight, including the Chief Information Officer's oversight of decision reviews.

Content of Software Resources Development Reports (SRDR)

- Contained on two pages of an Excel spreadsheet
- Consists of following five parts
  - Context
  - Product and Development Description
  - Size
  - Schedule and Effort
  - Quality

Content of Initial SRDR

- Part 1: Context
  - 1. System/Element Name (version/release)
  - 2. Report As Of Date
  - 3. Authorizing Vehicle (MOU, contract/amendment, etc.)
  - 4. Reporting Event: (Release start or project start)
  - 5. Name of Developing Organization
  - 6. Certified CMM Level (or equivalent)
  - 7. Certification Date
  - 8. Lead Evaluator
  - 9. Affiliation
  - 10. Precedents (list up to five similar systems by the same organization or team)
  - 11. Comments on part 1 responses

Content of Initial SRDR (Continued)

- Part 2: Product and Development Description
  - 1. For each application type involved: percentage of total, development process planned/used, and whether new or upgrade
    - Example application types include (from pre-defined list):
      - Real time command and control
      - Tactical Air Warfare
      - Communication
  - 2. Primary and secondary languages used
  - 3. List of COTS/GOTS planned
  - 4. Peak staff planned
  - 5. Percent of personnel planned that will be highly experienced, nominally experienced and entry level
  - 6. Comments for part 2 responses

Content of Initial SRDR (Continued)

- Part 3:Product Size
  - 1. Number of Software Requirements, not including External Interface Requirements
  - 2. Number of External Interface Requirements (i.e., not under project control)
  - 3. Code Size Measures for items 4 through 6. For each, indicate S for physical SLOC (carriage returns); Snc for non-commented SLOC only; LS for logical statements; or provide abbreviation _____ and explain in Software Measurement Data Dictionary.
  - 4. Expected New Code to be developed and delivered (Size in _____)
  - 5. Expected Modified Code (Size in _____)
  - 6. Expected Unmodified Reused Code (Size in _____)
  - 7. Comments on part 3 responses

Content of Initial SPDR (Concluded)

- Part 4: Schedule and Effort
  - Expected Start and End Month after contract award and Total Labor Hours for each phase or activity (examples shown below)
  - 1. Software Requirements Analysis
  - 2. Software Architecture and Detailed Design
  - 3. Software Coding and Unit Testing
  - 4. Software Integration and System/Software Integration
  - 5. Software Qualification Testing
  - 6. Software Operational Test and Evaluation
  - 7. All Other Direct Software Engineering Development Effort
  - Comments of part 4 responses
- Part 5: Product Quality
  - None required for initial report

Content of Final SPDR

- As-built values for all data elements on initial report
- Same data elements as Initial SPDR, plus two additional elements:
  - Part 3: Product Size: Amount of Requirements Volatility Encountered During Development
  - Part 5: Product Quality
    - 1. Measured or computed Mean Time to Defect (MTTD) of serious or critical defects at time of product delivery
    - 2. Alternate definition of delivered reliability (as defined in data dictionary)
    - 3. Comments on part 5 responses