Certification and Accreditation Transformation Overview

Briefing to the Annual Computer Security Applications Conference
December 13, 2007

Sharon Ehlers
ICTG/Policy and Planning Division
C&ATransformation@dni.gov
https://www.intelink.gov/mypage/c&a

Agenda

- Challenge and Background
- Policy
- Implementation
- Training
- Transition
- Benefits and Results

Challenge and Background

Challenge

- **Find an *innovative* and *efficient* way to perform Certification and Accreditation (C&A) activities across the *National Security* Community.**

Background

- Joint kick-off meeting with over 600 attendees
  - Associate Director of National Intelligence and Chief Information Officer (ADNI&CIO)
  - Assistant Secretary of Defense (Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO)
  - The National Institute of Standards and Technology (NIST)
- Nontraditional approach to solving this problem
  - *Internet* collaboration forums
  - *Volunteer* tiger teams
  - *Multi-national* War Room Panel
  - Input from *across* the government, industry, and academia

Background (continued)

- Participation of over 1,000 individuals
  - Federal Government
  - Industry
  - Commonwealth Partners
- Tiger teams and working groups
  - Led by the Director of National Intelligence (DNI) led
  - Leveraging Committee on National Security Systems (CNSS) efforts

Seven Transformational Goals

- Define a *common set of trust (impact) levels* and adopt and apply them across the Intelligence Community (IC) and DoD. Organizations will no longer use different levels with different names based on different criteria.
- Adopt *reciprocity* as the norm, enabling organizations to accept the approvals by others without retesting or reviewing.
- Define, document, and adopt *common security controls*, using NIST Special Publication (SP) 800-53 as a baseline.
- Adopt a *common lexicon*, using CNSS Instruction 4009 as a baseline, thereby providing DoD and IC a common language and common understanding.
- Institute a *senior risk executive function*, which bases decisions on an *"enterprise" view of risk considering all factors*, including mission, Information Technology (IT), budget, and security.
- *Incorporate information assurance (IA) into Enterprise Architectures* and deliver IA as common enterprise services across the IC and DoD.
- Enable a *common process* that incorporates security within the "life cycle" processes and eliminates security-specific processes. The common process will be adaptable to various development environments.

Key Accomplishments

- **We are working to *bring together* parallel efforts across the Federal Government to resolve this issue**
  - **Ensuring our approach is integrated with current activities supported by:**
    - Committee on National Security Systems (CNSS)
    - National Institute of Standards and Technology (NIST)
    - Office of Management and Budget (OMB) Information Systems Security Line of Business (ISS LOB)
    - Program Manager Information Sharing Environment (PM-ISE)
    - Unified Cross Domain Management Office (UCDMO)
- **We are moving toward a *unified* Federal approach**

Key Accomplishments (continued)

- Now integrated and aligned with CNSS
  - Addressing *all* National Security Systems (NSS) and all National Security Information equities
  - Includes IC, DoD, *and* civil agencies
  - Updating and creating CNSS publications to reflect C&A Transformational goals
  - Leveraging CNSS policies vice creating separate IC-specific ones
- Continuing to work with NIST to “align and coordinate” respective efforts
  - NIST providing “advisory” support and “sanity checks” to Transformation efforts
  - C&A Transformation Team providing recommendations and updates to NIST for improvements

Key Accomplishments (continued)

- Integrating with OMB Information Systems Security Line of Business C&A Working Group effort
  - Findings and Recommendations Report to OMB
    - Improve quality and costs
  - Leveraging C&A Transformation efforts
  - Determining "best practices" across Federal Government
  - Establishing Shared Service Centers for C&A "services"

HUD	EPA	CNSS
NIST	Dept of Treasury	Dept of Interior
Dept of Justice	NASA	Small Business Administration
SEC	Dept of Transportation	DNI
FDIC	Dept of Commerce	Bureau of Public Debt

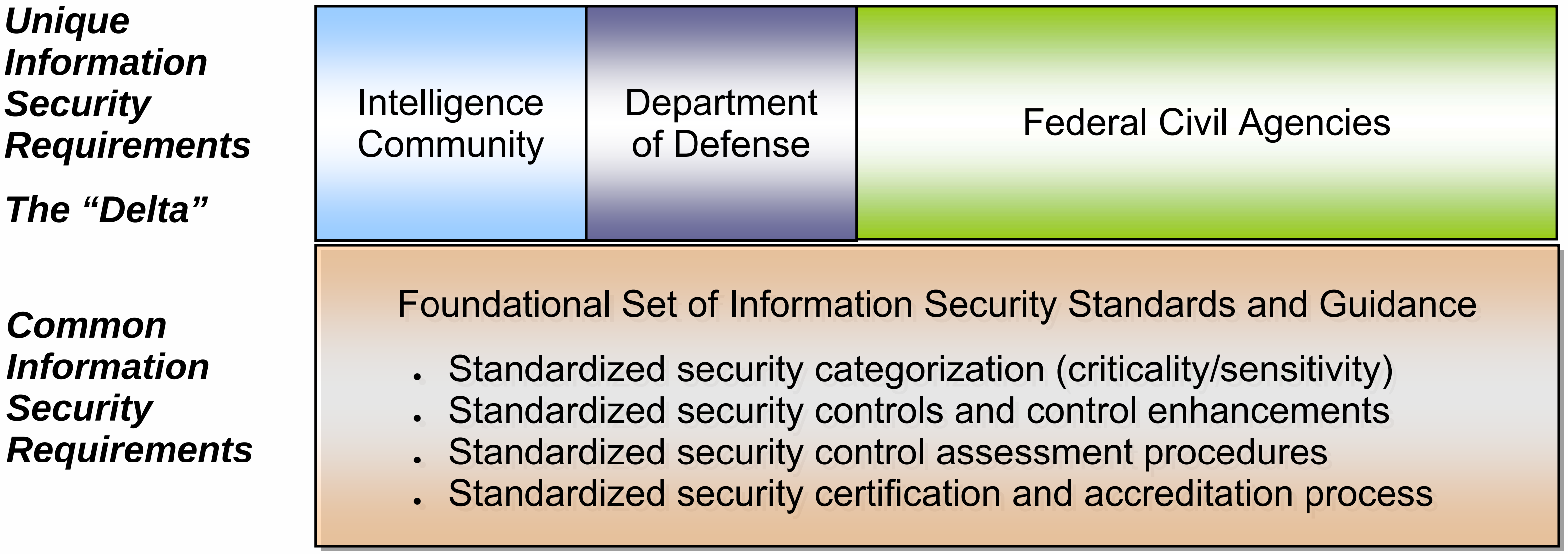
Key Accomplishments (continued)

- **Leveraging the Global Security Consortium (GSC) Department of Defense – Intelligence Community – Financial Sector Forum**
  - **Sharing "best practices" with financial sector**
    - Rapid integration of technology
    - Risk management

The Bank of New York	**UBS**	**Citigroup**
Depository Trust & Clearing Corporation	**Deutsche Bank**	**Goldman Sachs**
JPMorgan Chase	**Lehman Brothers**	**Merrill Lynch**
Morgan Stanley	**The NASDAQ Stock Market**	**Wachovia Corporation**

Governance and Policy

A Unified Framework



Unique Information Security Requirements

The "Delta"

Intelligence Community

Department of Defense

Federal Civil Agencies

Common Information Security Requirements

Foundational Set of Information Security Standards and Guidance

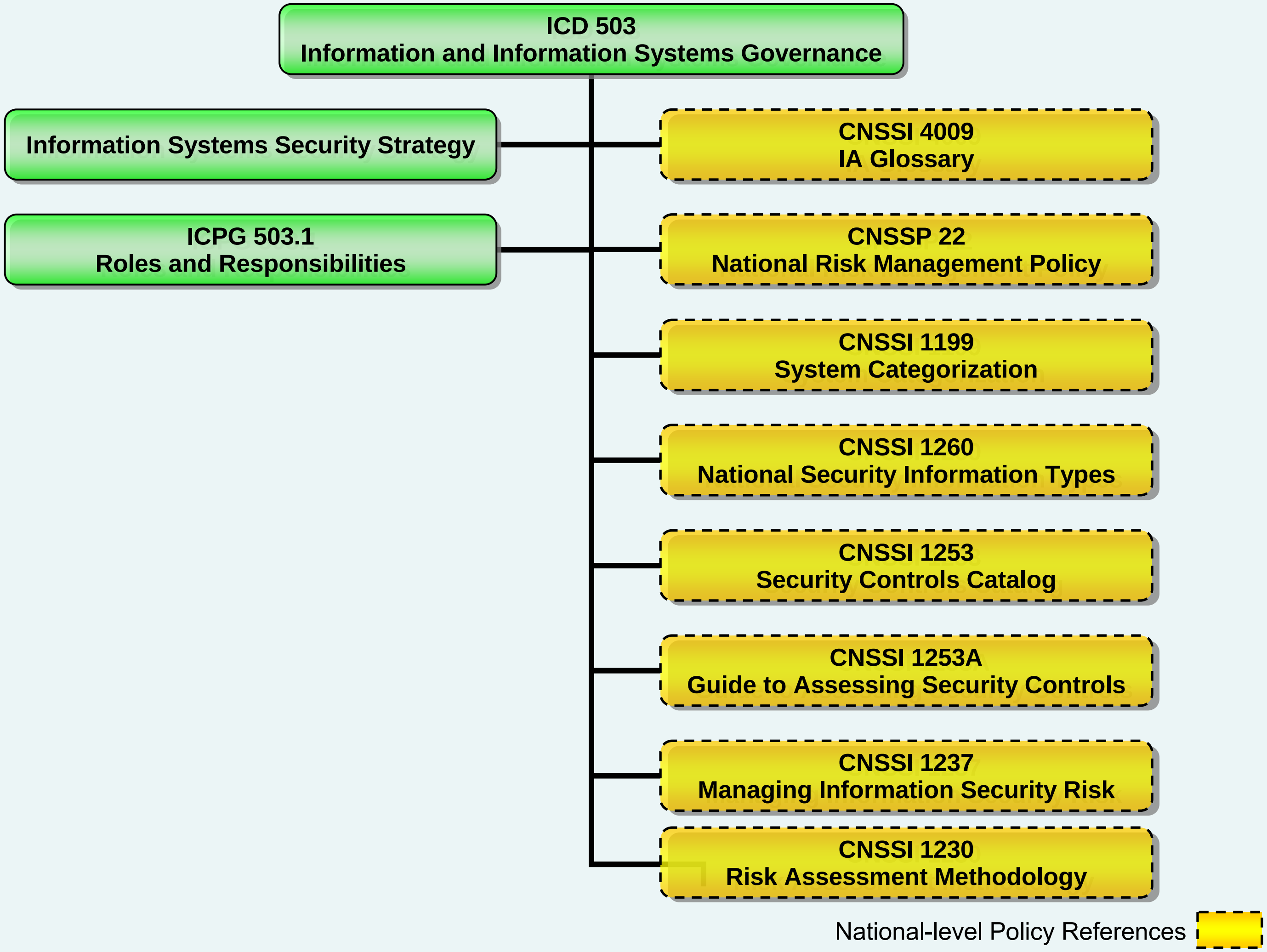
- Standardized security categorization (criticality/sensitivity)
- Standardized security controls and control enhancements
- Standardized security control assessment procedures
- Standardized security certification and accreditation process

National security and non-national security information systems

Approach to C&A Directives

- **Multifaceted approach to documentation**
  - **Drafting Intelligence Community Directive (ICD) and Intelligence Community Procedural Guides (ICPG)**
    - Outlines IC Information Security Program
  - **Leveraging existing NIST Special Publications as written**
    - Brings the IC closer to FISMA requirements
    - Assists with Inspector General (IG) audits, which are based on NIST standards
    - Aligns with rest of Federal Government to support reciprocity
  - **Where necessary, drafting CNSS supplements to Federal Information Processing Standards and NIST Special Publications**
    - Reflects "differences" for national security systems
      - System Categorization
      - Security Controls Catalog
      - Risk Management/Assessment

Proposed Policy Structure



ICD 503
Information and Information Systems Governance

Information Systems Security Strategy

ICPG 503.1
Roles and Responsibilities

CNSSI 4009
IA Glossary

CNSSP 22
National Risk Management Policy

CNSSI 1199
System Categorization

CNSSI 1260
National Security Information Types

CNSSI 1253
Security Controls Catalog

CNSSI 1253A
Guide to Assessing Security Controls

CNSSI 1237
Managing Information Security Risk

CNSSI 1230
Risk Assessment Methodology

National-level Policy References 🟨

Policy architecture now leverages national-level documentation

Implementation Approach

Addressing Risk from an Enterprise Perspective

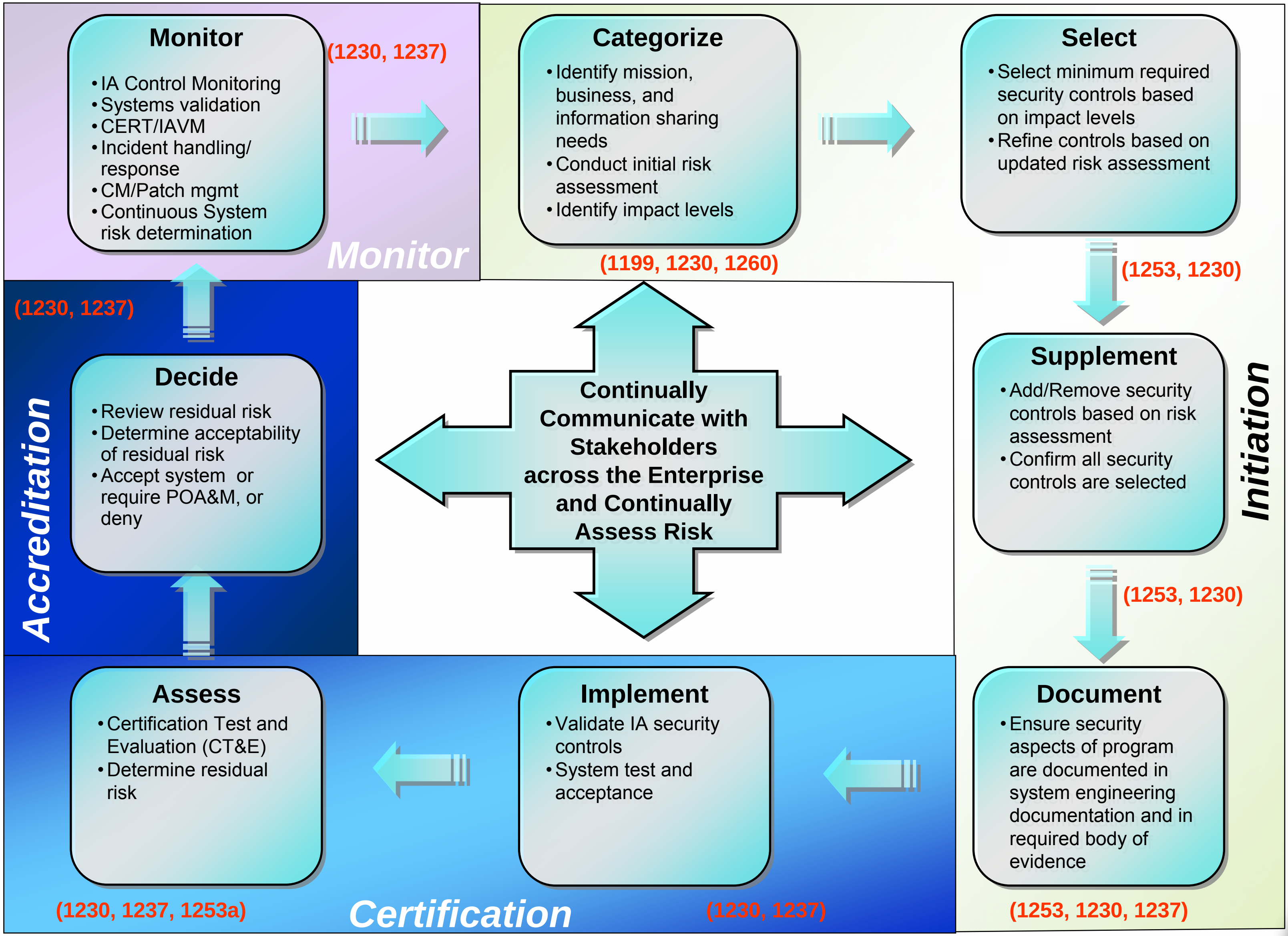
- **Key activities in managing enterprise-level risk***
  - ***Categorize*** **the information and systems (impact/criticality/sensitivity)**
  - ***Select*** **and tailor the security controls**
  - ***Supplement*** **the security controls based on risk assessment**
  - ***Document*** **the security controls as required essential information**
  - ***Implement*** **the security controls in the information system**
  - ***Assess*** **the security controls for effectiveness**
  - ***Decide*** **the enterprise/agency-level risk and risk acceptability and authorize information system operation**
  - ***Monitor*** **security controls on a continuous basis**

*** Risk resulting from the operation of an information system**

Roles

Authorizing Official	Makes ultimate risk decision to allow system to operate
Senior Risk Management Executive (function)	Provides enterprise-level risk assessment and maintains oversight to ensure holistic risk to the organization is considered at all phases of the life cycle.
Senior Agency Information Security Officer	Ensures agency compliance with information system security requirements and oversees agency Information Security Management Program
Certification Agent	Determines extent to which security controls are implemented correctly, operating as intended, and producing desired outcome
Program Manager/Mission Manager	Responsible for system meeting/maintaining its stated security requirements
Information Systems Security Engineer	Responsible for ensuring security requirements are properly handled and addressed throughout the development life cycle
Independent Validation Authority	Responsible for independent validation testing of security requirements and systems compliance
User Representative	Represents operational interests of the user community

C&A Phases and the Risk Management Framework



Monitor

- IA Control Monitoring
- Systems validation
- CERT/IAVM
- Incident handling/ response
- CM/Patch mgmt
- Continuous System risk determination

(1230, 1237)

Monitor

Categorize

- Identify mission, business, and information sharing needs
- Conduct initial risk assessment
- Identify impact levels

(1199, 1230, 1260)

Select

- Select minimum required security controls based on impact levels
- Refine controls based on updated risk assessment

(1253, 1230)

Supplement

- Add/Remove security controls based on risk assessment
- Confirm all security controls are selected

(1253, 1230)

Initiation

Document

- Ensure security aspects of program are documented in system engineering documentation and in required body of evidence

(1253, 1230, 1237)

Implement

- Validate IA security controls
- System test and acceptance

(1230, 1237)

Assess

- Certification Test and Evaluation (CT&E)
- Determine residual risk

(1230, 1237, 1253a)

Certification

Decide

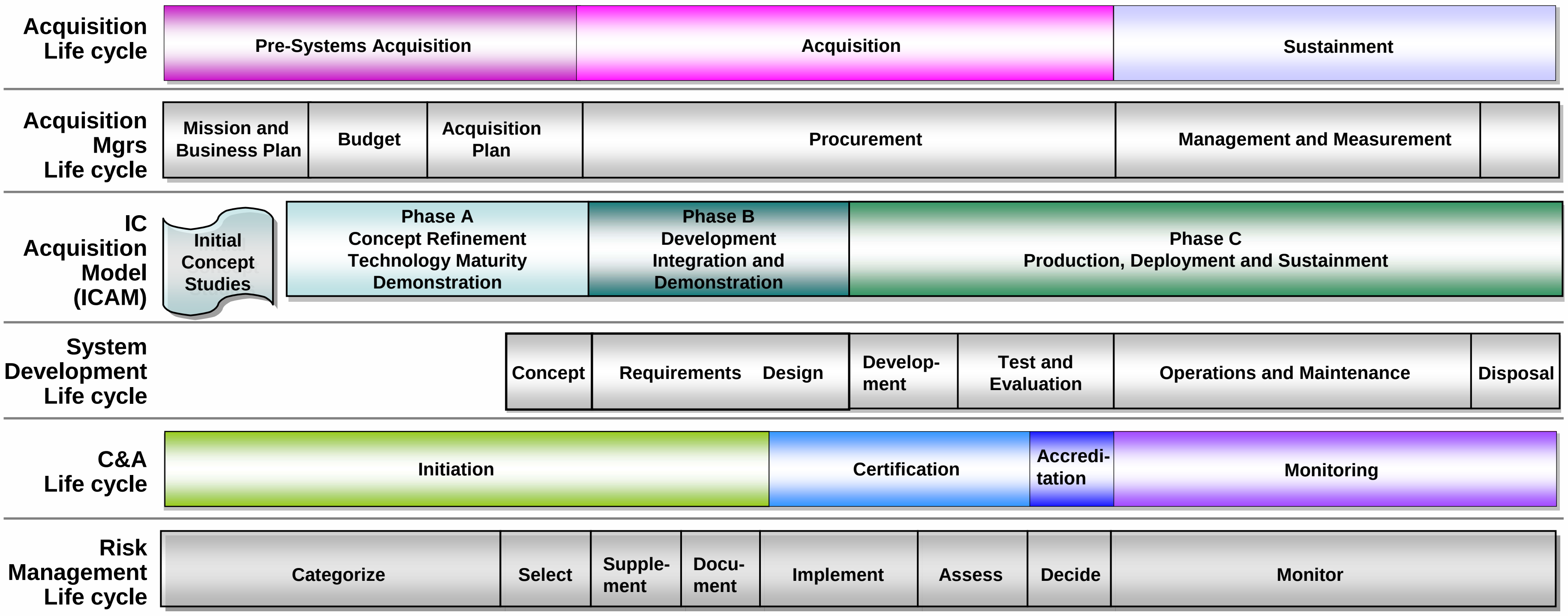
- Review residual risk
- Determine acceptability of residual risk
- Accept system or require POA&M, or deny

(1230, 1237)

Accreditation

Continually Communicate with Stakeholders across the Enterprise and Continually Assess Risk

Mapping C&A through Acquisition, SDLC, and the Risk Management Framework



Acquisition Life cycle: Pre-Systems Acquisition | Acquisition | Sustainment

Acquisition Mgrs Life cycle: Mission and Business Plan | Budget | Acquisition Plan | Procurement | Management and Measurement

IC Acquisition Model (ICAM): Initial Concept Studies | Phase A Concept Refinement Technology Maturity Demonstration | Phase B Development Integration and Demonstration | Phase C Production, Deployment and Sustainment

System Development Life cycle: Concept | Requirements Design | Development | Test and Evaluation | Operations and Maintenance | Disposal

C&A Life cycle: Initiation | Certification | Accreditation | Monitoring

Risk Management Life cycle: Categorize | Select | Supplement | Document | Implement | Assess | Decide | Monitor

Managing risk starts from the very beginning and continues throughout the life cycle. The Risk Management Framework can be applied at any level or function within the organization. C&A activities are tightly coupled to the Acquisition and System Development Life cycles

Minimizing but Improving C&A Documentation

- Future documentation requirements can be minimized if:
  - Engineering documentation also captures security functionality
  - Automated tools are utilized
  - Standardized templates are used across the Community
- Required Essential Information (REI) concept
  - Use what you need, when you need it, wherever it is located
- Baseline security documentation will include at least:
  - Security Assessment Report (SAR)
  - Plan of Actions and Milestones (POA&M)

Minimizing but Improving C&A Documentation (continued)

- Every document has a corresponding control and/or control enhancement
  - Amount or level of documentation for any given system is a key decision point early in the process and agreed to by all parties (no surprises!)
- Authorizing official will be required to “sign off” documentation throughout process to ensure management attention, document decisions, and provide accountability
- Revising statements of work (SOW) to ensure standardized deliverables

Maximizing Test Activities

- Integration of security personnel into program milestones ensures security activities are not “added on” but ‘built in”
  - Testing can be accomplished in years/months to weeks/days
- Use of automated tools will:
  - Streamline the evaluation of security controls, vulnerability scans, and penetration testing
  - Provide standardized test and evaluation templates
  - Build test case libraries to ensure reuse
- We are teaming with NIST, Department of Justice, Department of Energy, and Department of Treasury to build “assessment cases” for every security control
  - Developers will now have the ability to understand the requirement, know how to implement it, and know how it will be assessed

Use of Automation

- Automated tool enhances FISMA compliance, provides centralized reporting, automates work flow, and minimizes documentation
- Effort to establish tool “standards”
  - Would provide flexibility for agencies to use any automated tool that meets “standard” – GOTS or COTS
- Development of “tool kit” for Community use

Training

Training Is Critical to Success

- **Multipronged approach to training**
  - **Leveraging existing NIST training with modifications for national security systems specifics**
    - FISMA Phase 2 implementation
    - “Credentialing” of *assessors and assessment programs*

      SP 800-115 DRAFT Technical Guide to Information Security Testing
  - **Participating in OMB Tier II Training Working Group**
    - Addressing *individual* “certification” requirements
    - Findings and Recommendation Report to OMB

      Create a specific IT security job series, facilitating tracking of required training, metrics, and reporting

      Develop a Federal policy regarding certification for specific roles to advance the profession and provide baseline knowledge of key terms and concepts

Training Is Critical to Success (continued)

- **C&A Transformation Community Training Forum**
  - Five tracks
    - Acquisition/Contracting
    - IG/Legal
    - Executives/Senior Leadership
    - Security/Technical
    - Program Managers/Developers
- **Train the Trainer!**
  - Train organizations to further train their own staff/components

Transition

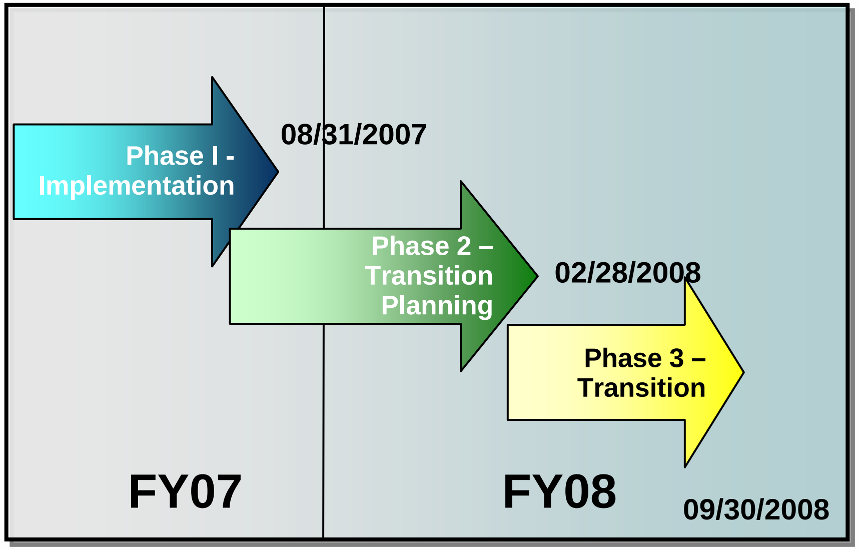
The Office of the Director of National Intelligence

Transition Planning Activities

Transition Activity	Proposed Due Date
Identify Agency Transition Manager	December 6, 2007
Identify a Transition Guidance Group Representative	December 6, 2007
Create an internal agency/ department C&A transition group	December 6, 2007
Begin attending Transition Guidance Group meetings	December 13, 2007
Draft Plan of Action and Milestones	First draft: January 7, 2008 Revised draft: February 7, 2008 Final: March 7, 2008

Transition Phased Approach

- **Phase 2 – Transition Planning**
  - **Duration: 6 months beginning September 2007**
    - Develop Transition Plan
    - Conduct impact and cost analyses
    - Coordinate agency, department, bureau transition
    - Assess and refine policies, guidance, and implementation
- **Phase 3 – Transition and Convergence**
  - **Duration: 7 months beginning March 2008**
    - Implement policies and guidance within organizations
    - Transition NSS community to providing common IA services
    - Converge and align NSS and non-NSS activities



Benefits and Results

Efficiencies Achieved

- General
  - A common approach and understanding
  - Full integration of security risk management with acquisition and business processes
  - Reliance on continuous monitoring
    - Going beyond “a snapshot in time” to obtain “real-world” security posture
- Local/Federated Enterprise Risk Views
  - A structured risk decision hierarchy
  - Ongoing risk evaluation and monitoring
  - Common framework and assessment methodology
  - Decisions include mission, budget, and security
  - Common definitions and terms

Building a New Security Culture

- Automated Standards-Based Tools
  - Ongoing and consistent security monitoring
  - Repeatable processes
  - Standard metrics
  - Remediation methods
  - Results that are useful to technicians and management
- Improved Management Insight
  - Ongoing, consistent, and understandable security communications
  - Greater understanding of risk
  - Management decisions based on REAL data
  - Ability to provide technical direction
- Professionalization of Security Workforce
  - Move from administrative to engineering functions

Providing Value-Added Results

- Certified connections within and between agencies and departments can be made in less time and with less effort
  - No longer need case-by-case evaluations and judgments
  - Maximize reuse of components and test data
- FISMA reports for department heads and OMB can be generated in half the time
- Security staff resources can be shifted from 80% administrative to 80% operational
- Technology can be deployed in days and weeks versus months and years

Contact Information

- **ODNI CIO C&A Transformation Team:**
  - Chief, ICTG/Planning and Policy Division: Sharon Ehlers, sharose@dni.gov, (703) 874-8125
  - Govt PM (C&A/CAT): Frank Sinkular, francijs@dni.gov, (703) 983-3340
  - Govt Rep (Tools): Dorian Pappas, dorianrp@dni.gov, (703) 983-1943
  - C&A Transformation Lead: Dan Klemm, danielrk@dni.gov, (703) 983-5470
  - C&A Transition Lead: Shelley Bard, sbard@mitre.org, (703) 983-4984
  - CAT Lead: Timothy Watt, tlwatt@tenacitysolutions.net, (703) 983-1765
- **Email address:**
  - Internet: C&ATransformation@dni.gov
- **Websites:**
  - Internet: http://www.dni.gov/dniwww/C&A.html
  - Intelink website: https://www.intelink.gov/mypage/c&a