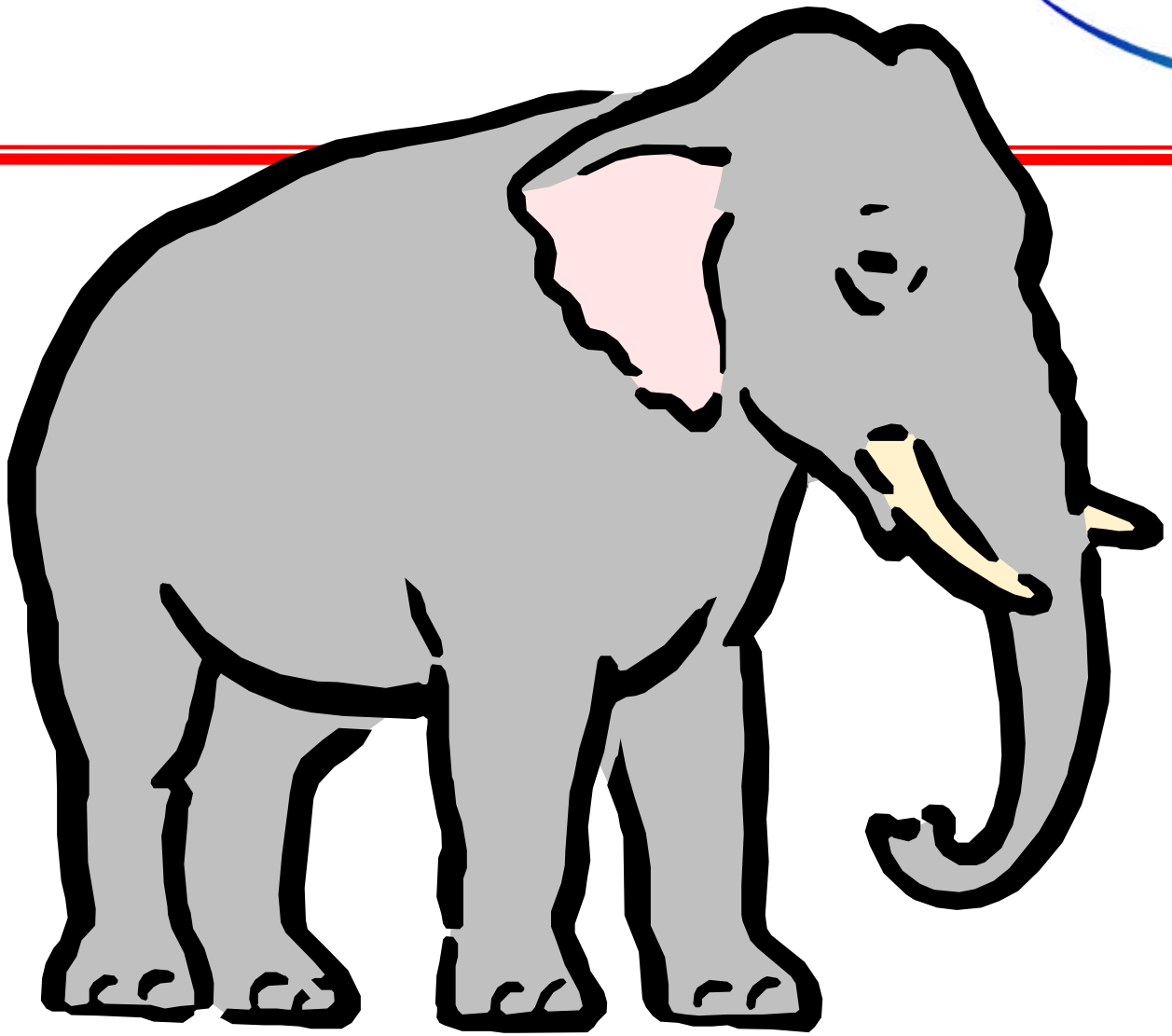
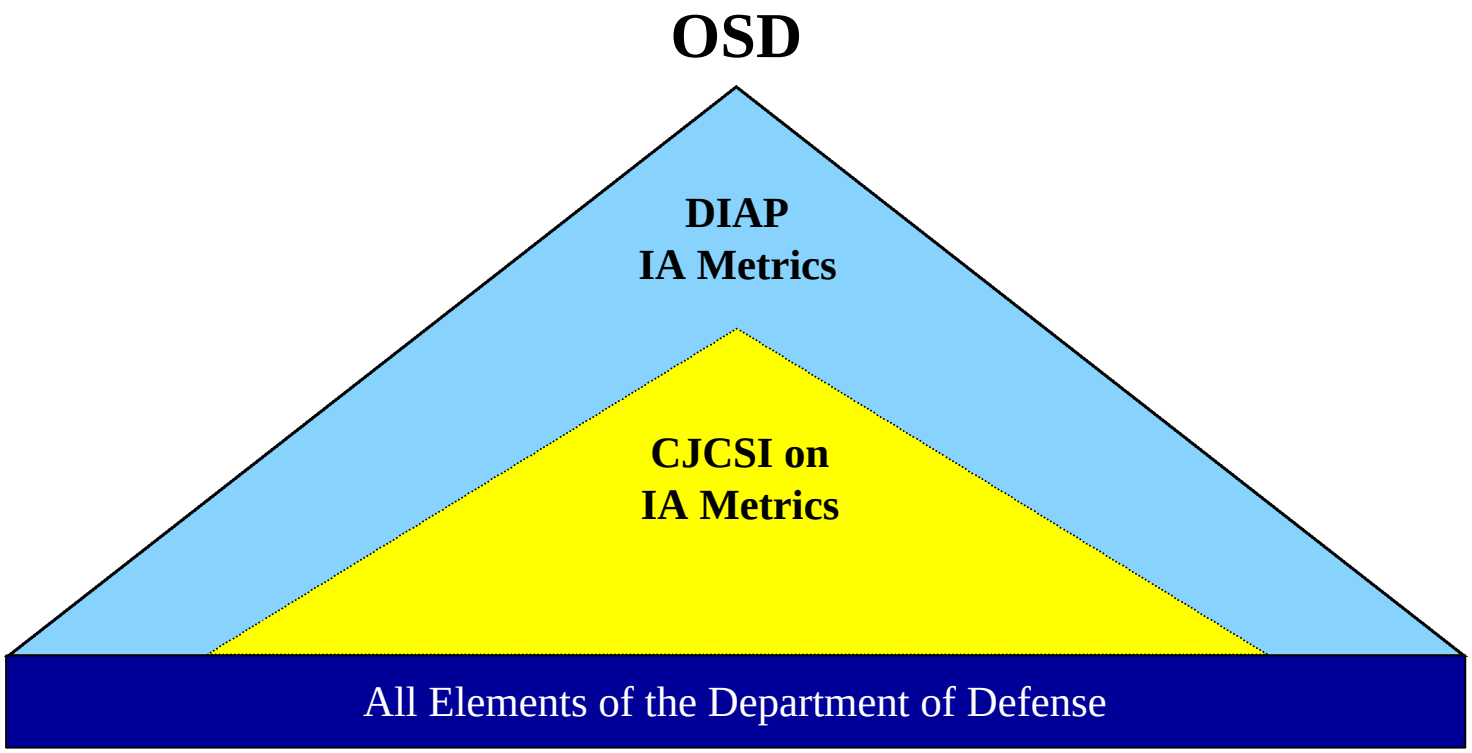
Information Assurance Readiness Assessment

Terry Bartlett, CISSP
Readiness Assessment Team Leader
703-602-9991
terry.bartlett@osd.pentagon.mil

IA Readiness Assessment



Assessment Framework



IA Readiness Assessment Tasking

- ASD(C3I) DIAP Implementation Plan (12 Feb 99)
  - Functional Evaluation and Integration Team
    - Consists of Eight Functional Areas
    - Develop IA Performance Goals, Standards, Metrics
    - Provide Oversight of Respective Functions
    - Ensure Coherent Integration Throughout DoD
  - Readiness Assessment Function
    - Member of Functional Evaluation and Integration Team
    - Provide Data Needed to Accurately Assess IA Readiness
    - IA Requirements Identification and Generation
    - Vulnerability/Threat Analysis, Assessment
    - Defense-Wide Standards and Readiness Reporting Systems

DIAP
Goal & Objectives

- Goal: Ensure a Comprehensive, Coherent IA Program Across the DoD
- Objective: Assess the state of DoD's IA Posture
- Tasks:
  - Ensure IA assessment is incorporated into the DoD Exercise program
  - Develop business case and methodology for IA damage assessment
  - Establish appropriate metrics

DIAP
Goal & Objectives

- Sub-Tasks:
  - Develop appropriate and useful metrics
  - Validate metrics
  - Cost out the metrics collection processes
  - Obtain approval from appropriate sources for metrics collection
  - Deploy DOD-wide process for reporting IA metrics

Readiness Assessment Goal & Objectives

- Goal: Operationalize IA Readiness
- Objectives:
  1. Define IA Readiness in Operational Context
  2. Establish Metrics for Measuring IA Readiness
  3. Establish Standard Criteria for Applying IA Readiness Metrics
  4. Establish IA Readiness Assessment Process
  5. Integrate IA Readiness Assessment into Existing DOD Processes

Challenges

- IA Effectiveness is Not Currently Measured
  - Must structure IA Readiness Assessment to ensure sufficient protection of the information component of our war fighting resources
  - Must Build IA assessment into existing DOD processes
- IA has Limited Visibility in the PPBS Process
  - Must make IA Readiness fiscally defensible
  - Must make an effective Business Case for IA

Challenges

- Breaking New Ground with IA Readiness
- Primary Stakeholders Must Work Together
  - Operational Readiness Community
  - Information Assurance Community
- Everyone's Looking for Solutions
  - No Commonly Accepted IA Metrics
  - No Commonly Accepted IA Assessment Process
    - Continuing Debate Over Process Review Vs Audit
- There is No Perfect Solution
  - Process Must Include Iterative Review and Update

Challenges

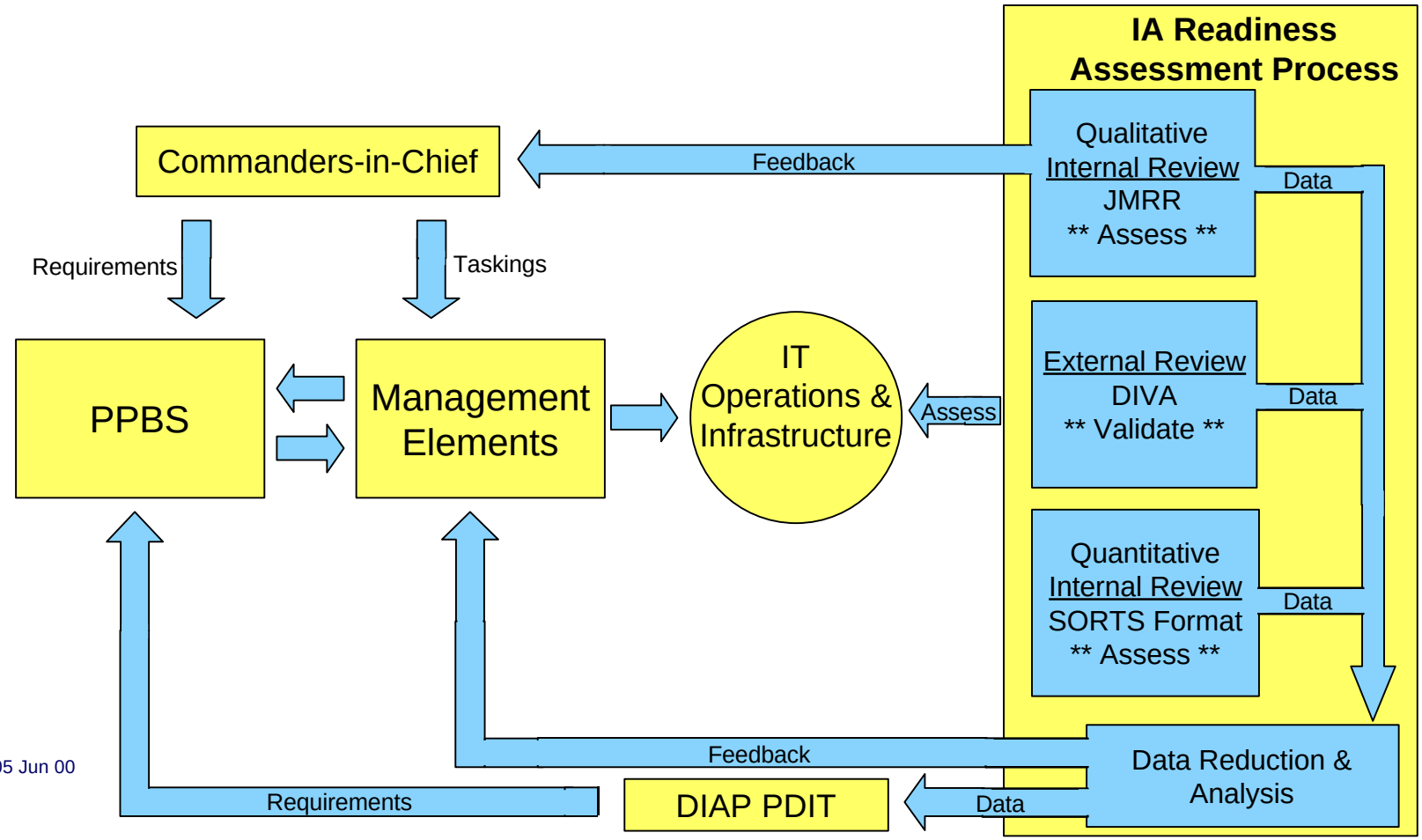
- Information Assurance Readiness Assessment Will Affect Everyone
  - Combat Forces and Combat Support Agencies
- Results Must be Accepted Throughout DOD
  - Readiness Stakeholders and IA Stakeholders
  - Combat Forces and Combat Support Agencies

Assessment Framework

Proposed Definition of IA Readiness

"The measured ability of DOD information technology systems, embedded information technologies, and their related infrastructures to withstand incidents and attacks, and provide effective support to execution of the Department's combat and non-combat missions."

Assessment Framework Concept



Assessment Framework Concept

- To Ensure Success, Assessment Process Must Be:
  - Consistent
    - Standard Metrics Should be Composites to Adequately Measure "Areas of Interest" Across DoD
    - Metrics Should Be Unchanging for Incorporation into Permanent Processes
  - Flexible
    - Criteria will Apply Standard Metrics Across Diverse Environments
      - Provides Method to Change "Content" of Metrics, but not Meaning
    - Changes to Criteria Affect Data Considerations, Not Processes
  - Relevant
    - Should Facilitate Analysis to Forecast Capabilities, Effectiveness and Requirements
    - Metrics are Not Merely Statistics

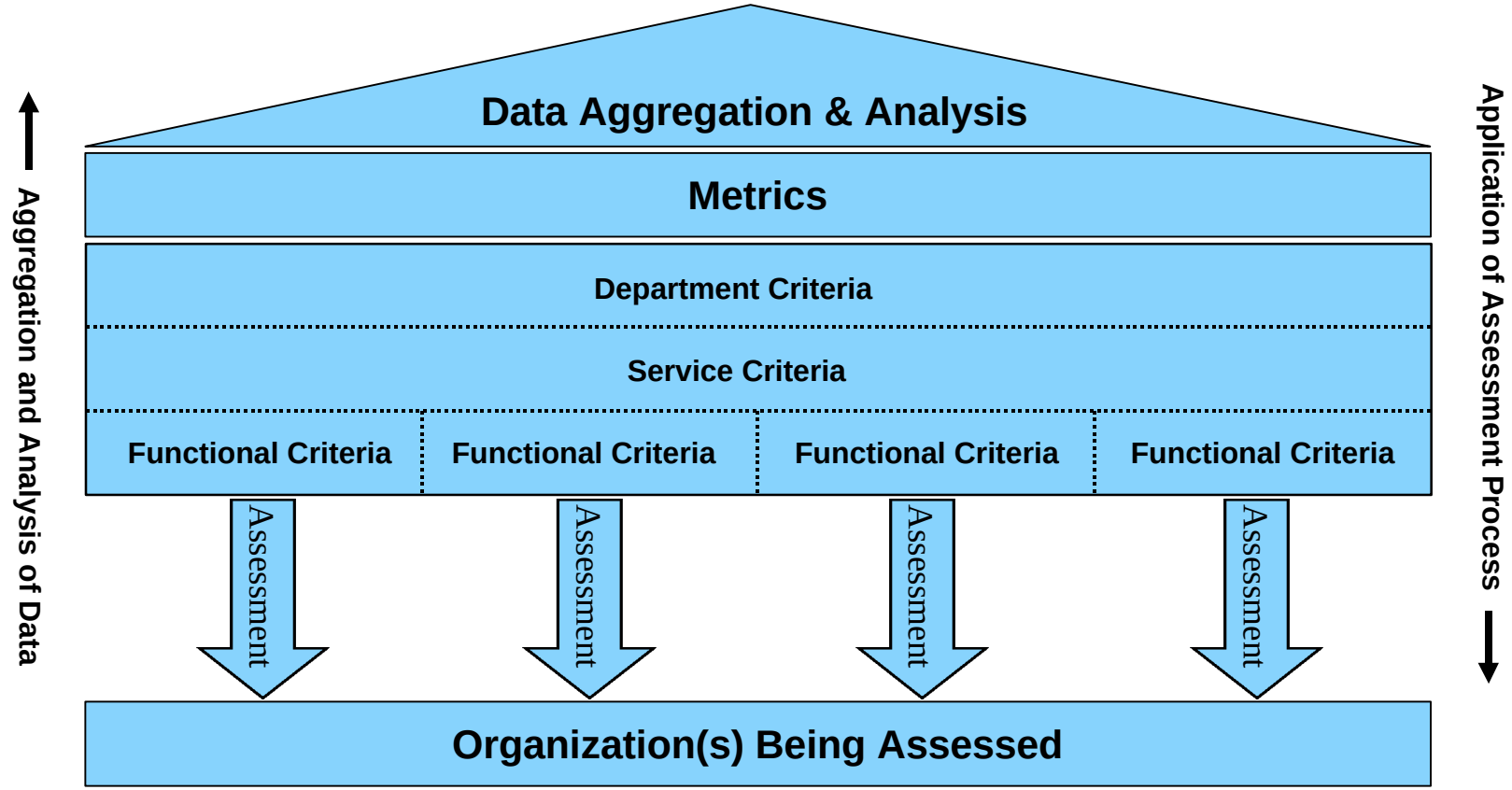
Assessment Framework

- Examples of Widely-Used Consistent, Flexible Metrics:
  - Dow Jones Industrial Average
  - Gross Domestic Product
  - Consumer Price Index
  - Unemployment Index
- Characteristics of Example Metrics:
  - Each Metric has a Formula, or Criteria, for Its Application
    - Consists of a Quantity of Elements, Each with a Weighting Factor
  - Can Nominally Change Each Metric's Formula Without Changing Its Meaning
    - Everyone Understands What the Metrics Represent

Assessment Framework Concept

- Three Levels of Criteria Used in Notional Framework:
  - Department Criteria
    - Statement of DoD Policy & Guidance
    - Specifies Highest-Level Parameters for Metrics
  - Service Criteria
    - Regulations, Instructions Implementing DoD Policy
    - Applies Service Considerations To Metrics
  - Functional Criteria
    - Affects Assets Assigned to Support Respective Functional Areas
    - Specifies Mission-Oriented Requirements & Constraints for Assessed Systems

Assessment Framework Concept



Assessment Framework Metrics Scoring

- Metric Scores are Same as in SORTS (C1, C2, C3, C4)

Rating	C-Rating		Graphic
Excellent	C1	=	G
Acceptable	C2		
Marginal	C3	=	Y
Unacceptable	C4	=	R

Assessment Framework Metrics Map

Category	Metric	Availability	Integrity	Confidentiality	Authentication	Non-Repudiation
People	Adequacy of Critical IT/IA Staff Manning Levels	X	X	X		
	Adequacy of Critical IT/IA Staff Proficiency	X	X	X	X	X
	Adequacy of Security Clearances for Privileged Users	X	X	X		
	Effectiveness of Information Systems Security Program	X	X	X	X	
Operations and Training	Adequacy of Fail Over Testing for Mission Critical Systems	X	X	X		
	Adequacy of Performance Measurement for Network Infrastructure and Mission Critical Systems	X	X			
	Effectiveness of Network Penetration Detection and Defense Capabilities	X	X	X	X	
	Effectiveness of Network Management Auditing Program	X	X	X	X	X
	Effectiveness of Firewall Administration Practices, Procedures, and Compliance	X	X	X	X	X
	Adequacy of Requirements for IT Contractor Support	X	X	X	X	
	Effectiveness of IA Vulnerability Alert Procedures	X	X	X	X	
Equipment and Infrastructure	Adequacy of Technology to Support Assigned Missions	X	X	X	X	
	Adequacy of Bandwidth to Support Mission Critical Systems	X	X			
	Adequacy of Connectivity Robustness for Mission Critical Systems	X	X			
	Adequacy and Effectiveness of Survivable Power	X	X	X		
	Adequacy and Effectiveness of Facility Security Systems, Practices, and Procedures	X	X	X	X	
	Adequacy and Effectiveness of Entry Control Systems for Mission Critical and Infrastructure Facilities	X	X	X		

Assessment Framework Notional Metrics Criteria

Category	Metric (Aggregated)	Metric (Non-Aggregated)	OSD Criteria	Service Criteria	Rating	Criteria for C2 Function
People	Adequacy of IA Personnel Manning Levels	Adequacy of IA Personnel Manning Levels	1. All IA billets must be designated per DoD policy xxxx 2. All IA billets must be accounted for	The following billets are identified as IA billets	C1	90% manned, replacements identified for outbound personnel
					C2	90% manned, replacements not identified for outbound personnel
					C3	75% to 89% manned
					C4	Less than 75% manned
	Adequacy of IA Personnel Proficiency	Adequacy of IA Operations Personnel Proficiency (Maps to Adequacy of IA Personnel Proficiency Metric)	Operations personnel must be trained and certified by cognizant authority for system(s) they are responsible for	The following billets are identified as IA operations billets	C1	All operations personnel have received xx hours of training in last 3 months
					C2	All operations personnel have received xx hours of training in last 6 months
					C3	Some personnel have received no training in last 6 months
					C4	Some operations personnel are not certified to perform their duties

Assessment Framework Notional Metrics Criteria

Category	Metric (Aggregated)	Metric (Non-Aggregated)	OSD Criteria	Service Criteria	Rating	Criteria for C2 Function
People	Adequacy of IA Personnel Proficiency	Adequacy of IA Maintenance Personnel Proficiency (Maps to Adequacy of IA Personnel Proficiency Metric)	Maintenance personnel must be trained and certified by cognizant authority for system(s) they are responsible for	The following billets are identified as IA maintenance billets	C1	80% or more of assigned IA maintenance personnel are mid-skill level qualified or above
					C2	70% or more of assigned IA maintenance personnel are mid-skill level qualified or above
					C3	60% or more of assigned IA maintenance personnel are mid-skill level qualified or above
					C4	Less than 60% of assigned IA maintenance personnel are mid-skill level qualified or above
		Adequacy of Information Systems Security Office Personnel Proficiency (Maps to Adequacy of IA Personnel Proficiency Metric)	ISSO personnel must be trained and certified by cognizant authority	The following billets are identified as ISSO billets	C1	All assigned ISSO personnel have completed formal training and been certified
					C2	Some assigned ISSO personnel have completed formal and/or informal training but not been certified
					C3	Some assigned ISSO personnel have completed no formal and/or informal training
					C4	No assigned ISSO personnel completed any formal and/or informal training

Assessment Framework Notional Metrics Criteria

Category	Metric (Aggregated)	Metric (Non-Aggregated)	OSD Criteria	Service Criteria	Rating	Criteria for C2 Function
People	Adequacy of Security Clearances for Privileged Users	Adequacy of Security Clearances for Privileged Users	1. All privileged user billets must be designated per DoD policy xxxx 2. All privileged users must be cleared for the classification of the system they have access to	The following billets are identified as privileged user billets/positions	C1	TBD
					C2	TBD
					C3	TBD
					C4	TBD
	Effectiveness of Information Systems Security Program	Effectiveness of Information Systems Security Program	Each IS Security Program must have a charter explicitly promulgated by the installation commander or equivalent	TBD	C1	TBD
					C2	TBD
					C3	TBD
					C4	TBD

Assessment Framework Notional Metrics Criteria

Category	Metric (Aggregated)	Metric (Non-Aggregated)	OSD Criteria	Service Criteria	Rating	Criteria for C2 Function
Operations and Training	Adequacy of Automatic/Manual Fail Over Testing for Mission Critical Systems	Adequacy of Automatic/Manual Fail Over Testing for Mission Critical Systems	All mission critical back-up systems must provide capabilities as designed, as required, and within applicable constraints	The following systems are designated as mission critical back-up systems	C1	All systems have auto-fail over capability and were tested successfully within the last month
					C2	All systems have auto-fail over capability and were tested successfully within the last 2 months
					C3	All systems have auto-fail over capability and were tested successfully within the last 3 months
					C4	All systems have auto-fail over capability and were not tested successfully within the last 3 months, or some have no auto-fail over capability
	Adequacy of Performance Measurement for Network Infrastructure and Mission Critical Systems	Adequacy of Performance Measurement for Network Infrastructure and Mission Critical Systems	All systems must meet or exceed operational availability requirements	Reference applicable system requirements documents for operational availability requirements	C1	TBD
					C2	TBD
					C3	TBD
					C4	TBD

Assessment Framework Notional Metrics Criteria

Category	Metric (Aggregated)	Metric (Non-Aggregated)	OSD Criteria	Service Criteria	Rating	Criteria for C2 Function
Operations and Training	Effectiveness of Network Penetration Detection and Defense Capabilities	Effectiveness of Network Penetration Detection and Defense Capabilities	Procedures must be in place & use to respond to and report network penetration activities		C1	TBD
					C2	TBD
					C3	TBD
					C4	TBD
	Effectiveness of Network Management Auditing Program	Effectiveness of Network Management Auditing Program	Procedures must be in place & use for Continuity of Ops; disaster recovery planning; risk detection & mitigation; use of updated software patches; and use of updated anti-virus software and signatures		C1	Perform random audits to measure network security policy compliance. 100% of nets have been audited in last year, 25% in last 3 months
					C2	Perform scheduled audits to measure network security policy compliance. 100% of nets have been audited in last year, 25% in last 3 months
					C3	Perform random or scheduled audits to measure network security policy compliance. LT 100% of nets have been audited in last year, with 25% occurring in last 3 months
					C4	Less than 25% of installation nets have been audited in last 3 months

Assessment Framework Notional Metrics Criteria

Category	Metric (Aggregated)	Metric (Non-Aggregated)	OSD Criteria	Service Criteria	Rating	Criteria for C2 Function
Operations and Training	Effectiveness of Firewall Administration Practices, Procedures, and Compliance	Effectiveness of Firewall Administration Practices, Procedures, and Compliance	Firewalls must not be in factory default configuration		C1	Duties performed by dedicated personnel with formal training
					C2	Duties performed as extra-duty by personnel with formal training
					C3	Duties performed by dedicated personnel without formal training
					C4	Duties performed as extra-duty by personnel without formal training
	Adequacy of Requirements for Contractor Support	Adequacy of Requirements for Contractor Support	Consideration must be given to the following contractual items: Response times, minimum qualifications, performance guarantees, security clearances, etc..		C1	TBD
					C2	TBD
					C3	TBD
					C4	TBD

Assessment Framework Notional Metrics Criteria

Category	Metric (Aggregated)	Metric (Non-Aggregated)	OSD Criteria	Service Criteria	Rating	Criteria for C2 Function
Operations and Training	Effectiveness of Information Assurance Vulnerability Alert Procedures	Effectiveness of Information Assurance Vulnerability Alert Procedures	All DoD elements must comply with IAVA compliance and reporting requirements		C1	All required actions have been accomplished, and 100% were within time constraints
					C2	All required actions have been accomplished, and 80% were within time constraints
					C3	All required actions have been accomplished, and 60% were within time constraints
					C4	All required actions have not been accomplished
Equipment and Infrastructure	Adequacy of Technology to Support Assigned Mission	Adequacy of Technology to Support Assigned Mission	Consideration must be given to the following items: Age of equipment; and age, capability, robustness of crypto, etc..		C1	TBD
					C2	TBD
					C3	TBD
					C4	TBD

Assessment Framework Notional Metrics Criteria

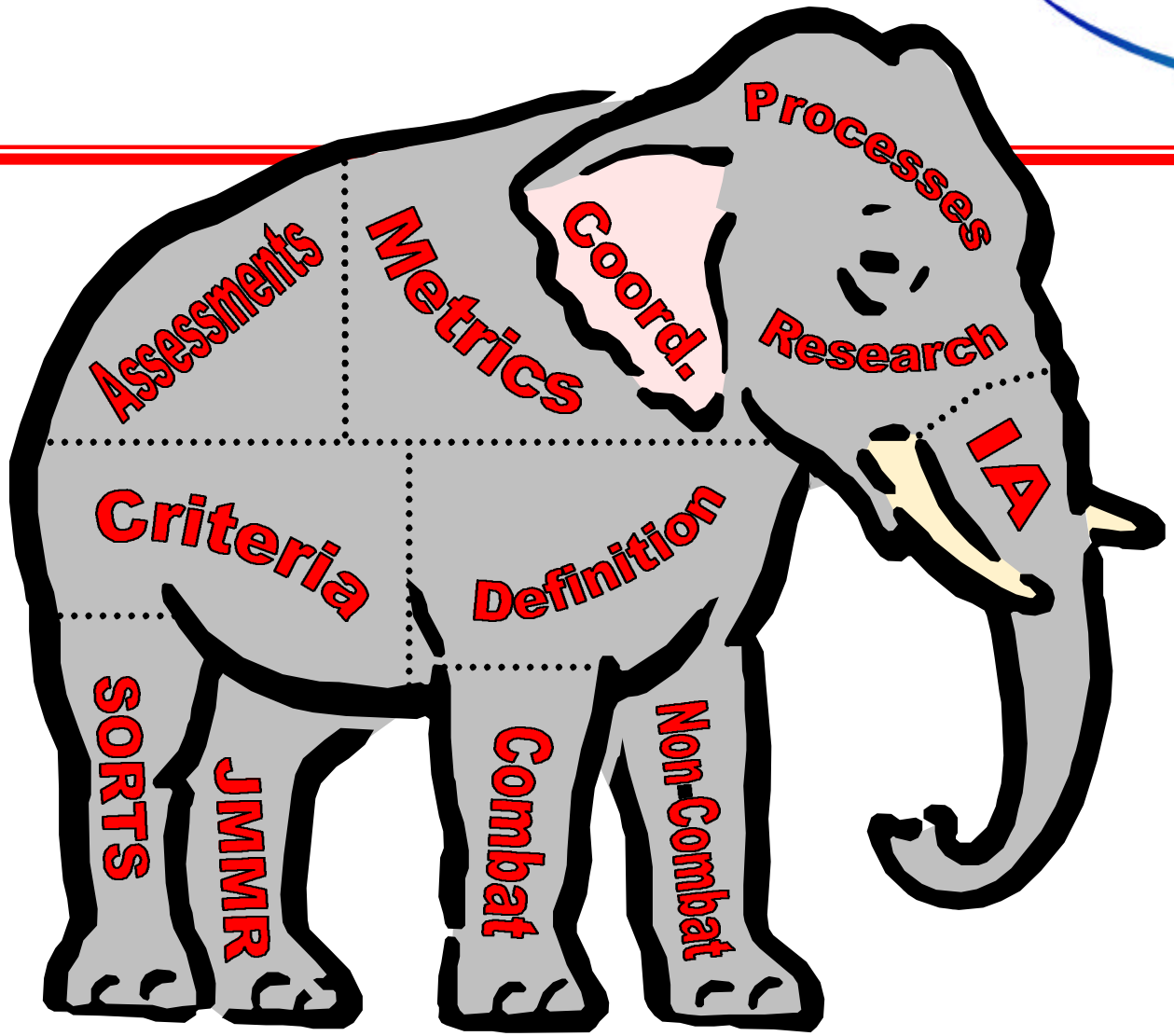
Category	Metric (Aggregated)	Metric (Non-Aggregated)	OSD Criteria	Service Criteria	Rating	Criteria for C2 Function
Equipment and Infrastructure	Adequacy of Bandwidth to Support Assigned Mission Critical Systems	Adequacy of Bandwidth to Support Assigned Mission Critical Systems	All DoD elements must measure bandwidth for all assigned systems that compete with mission critical systems for bandwidth resources	The following systems are designated Mission Critical Systems	C1	Installation has sufficient bandwidth such that normal utilization consumes a max of 40% and projected surge is less than 70% of available
					C2	Installation has sufficient bandwidth such that normal utilization consumes a max of 60% and projected surge is less than 80% of available
					C3	Installation has sufficient bandwidth such that normal utilization consumes a max of 80% and projected surge is less than 90% of available
					C4	Normal utilization consumes more than 80% or projected surge is greater than 90% of available
	Adequacy of Connectivity Robustness to Support Assigned Mission Critical Systems	Adequacy of Connectivity Robustness to Support Assigned Mission Critical Systems	TBD	TBD	C1	All systems have dual circuits available, with dual routing, and no known single points of failure
					C2	All systems have dual circuits available, with dual routing, and known single points of failure
					C3	All systems have dual circuits available, without dual routing
					C4	One or more systems are single threaded

Assessment Framework Notional Metrics Criteria

Category	Metric (Aggregated)	Metric (Non-Aggregated)	OSD Criteria	Service Criteria	Rating	Criteria for C2 Function
Equipment and Infrastructure	Adequacy and Effectiveness of Survivable Power	Adequacy and Effectiveness of Survivable Power	TBD	TBD	C1	Systems have auto-switching power that tested successfully in last 3 months
					C2	Systems have auto-switching power that tested successfully in last 6 months
					C3	Systems have auto-switching power that tested unsuccessfully in last 6 months
					C4	Systems have auto-switching power not tested in last 6 months, or no auto-switching power
	Adequacy and Effectiveness of Facility Security Systems, Practices, and Procedures	Adequacy of Connectivity Robustness to Support Assigned Mission Critical Systems	TBD	TBD	C1	Facility is patrolled, fenced, lighted, and has intrusion alarm system
					C2	Facility is patrolled, fenced, and lighted
					C3	Facility is patrolled and fenced
					C4	Facility has no perimeter protection
	Adequacy and Effectiveness of Entry Control Systems for Mission Critical and Infrastructure Facilities	Adequacy and Effectiveness of Entry Control Systems for Mission Critical and Infrastructure Facilities	TBD	TBD	C1	TBD
					C2	TBD
					C3	TBD
					C4	TBD

Activities
Current & Forthcoming

- Continue Development of Strawman Framework
- Readiness Assessment Workshop 12-14 July 2000
  - DoD Agency, Service, Joint Staff and CINC Participation
  - Formalize Assessment Framework
- Draft Implementing Guidance
- Beta Test

IA Readiness Assessment

"One Bite at A Time"