Overview of Information Assurance (U)

Dr. Theodore Mueller
Deputy Director, DOCV
Missile Defense Agency

September 1, 2009

Information Assurance (U)

- **Definition – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities**

Three MDA Networks:

1. **Mission** – Network directly supporting the missile defense operational mission, i.e., directly contributes to target identification and missile launch
2. **Test** – Network indirectly supporting the operational mission, i.e., test network, assists the Warfighter
3. **GENSER** – Network supporting administrative classified and unclassified users

BMDS View

Legend
SA : Strategic Awareness
FC: Fire Control
Phase of BMDS
Goal of Protection

War Fighter NORTHCOM

War Fighter PACOM

War Fighter STRATCOM

SA
FC

C2BMC

C2BMC

C2BMC

Boost

Mid-Course

Terminal

Home

Allies

Troops

ABL Element

GMD Element

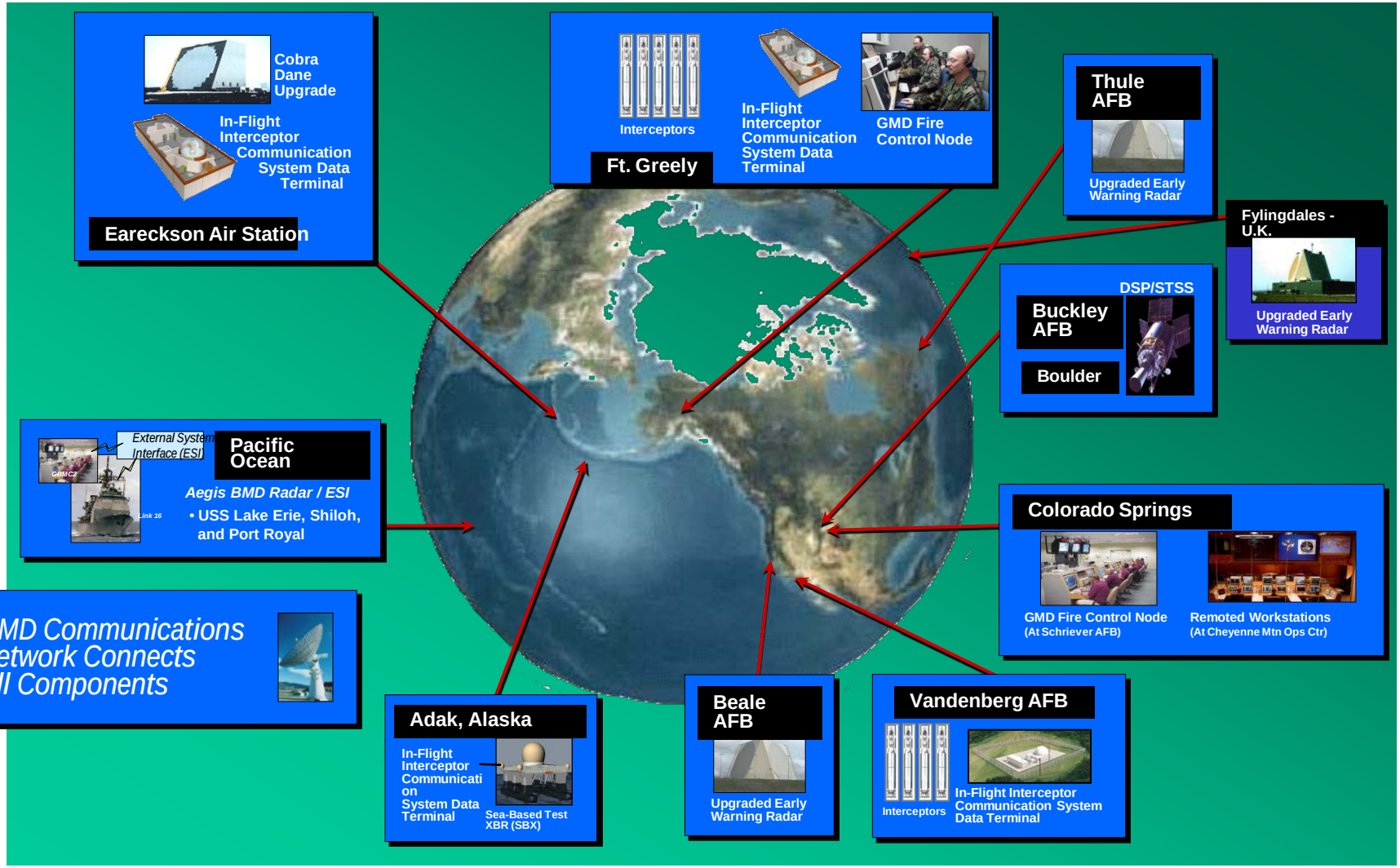
THAAD Element

Test Network

Labs

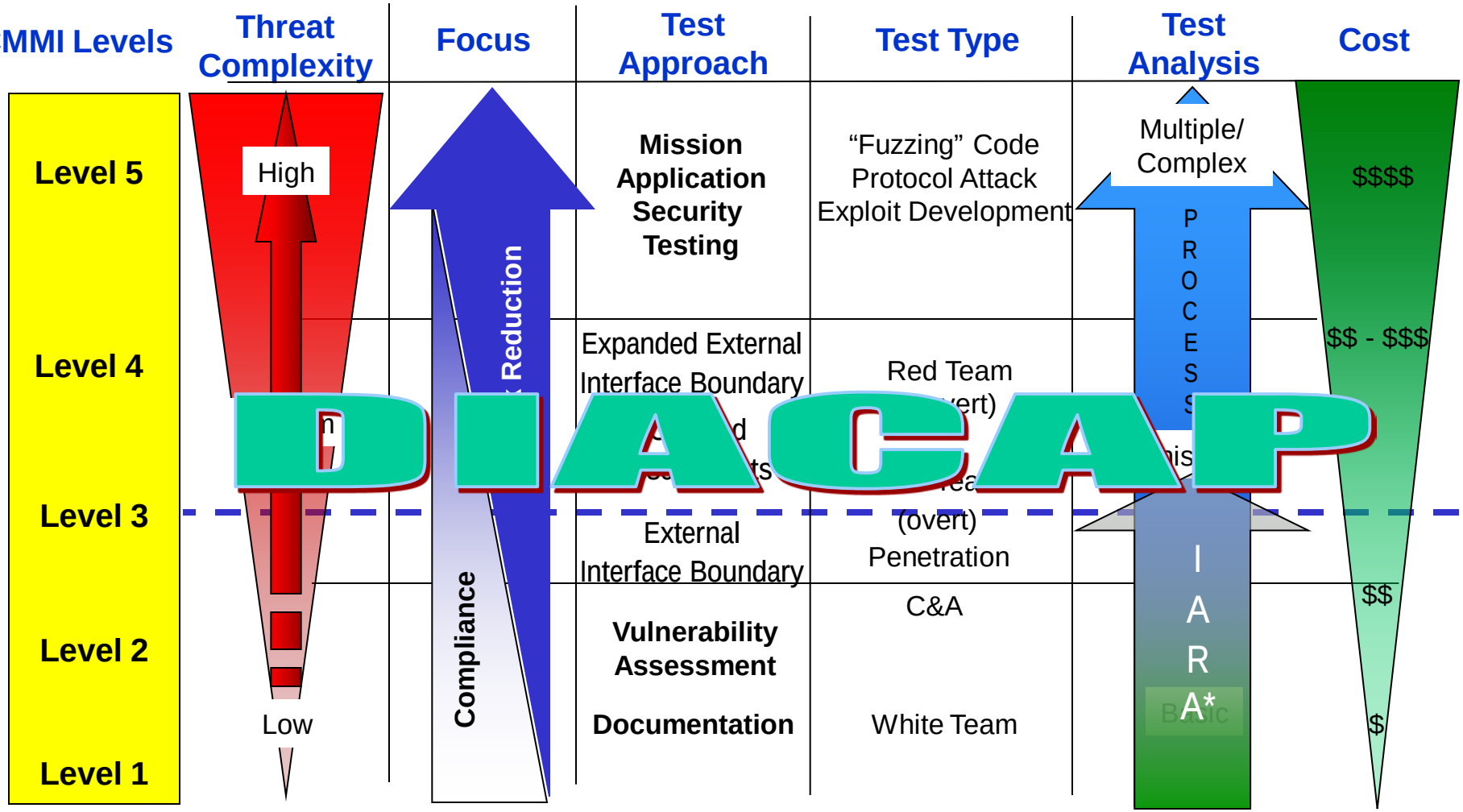
Range

MDA Mission is Worldwide (GMD Example)



MDA C&A Process Concept

IA Capability Maturity Model Integrated (CMMI)



Defined, Disciplined, Repeatable, and Defendable Process

Potential Business Opportunities

Current Contractor: Dynetics – value at approximately $6.5m

Key requirement – perform functions better, cheaper, and more efficiently:

Testing (Defense Information Assurance Certification and Accreditation Process (DIACAP)) –

- **Better** – more sophisticated test tools, scenario driven tests, tools that identify malicious code
- **Cheaper** – remote testing tools instead of deploying test teams
- **Efficient** – tools that combine results of other tools, automated analysis

Training (DoD 8570.01) –

- **Better** – combine classroom, hand's-on, tailored, multi-levels
- **Cheaper** – distant learning, export via CD or Web
- **Efficient** – centralized management, decentralized execution

Summary

- **Information Assurance is mandated, growing in importance and here to stay**
- **Business opportunities exist in identifying key IA activities or processes and offering a way to perform them better, cheaper, and more efficiently**
- **Key activities include:**
  - **Testing**
  - **Analysis**
  - **Develop IA certification & Accreditation packages**
  - **Training**
  - **Tools**
  - **Archiving artifacts, findings, etc.**

Cost Benefit Analysis must justify Government action to contact


MISSILE DEFENSE AGENCY
DEPARTMENT OF DEFENSE

BACKUP

Controls Validation Testing

- **Mandatory legal requirement under Title 10, US Code, Section 2224, OMB Circular A-130, and DOD regulations and policies**
- **110 Information Assurance (IA) Controls are tested resulting in:**
  - **No finding – Tested IA Control is compliant**
  - **CAT I allows primary security protections to be bypassed, allowing immediate access by unauthorized personnel. Any identified weaknesses must be mitigated within 30 days**
  - **CAT II – has the potential to lead to unauthorized system access or activity**
  - **CAT III – may impact IA posture but are not required to be mitigated in order to receive an Authority to Operate**

Certification and Accreditation Decisions

- **Interim Authorization to Test - IATT**
  - Special case for authorizing testing in an operational informational environment (pre-deployment / test environment)
  - Specified period of time
- **Authorization to Operate - ATO**
  - Applies only to operationally ready information systems (operational environment)
- **Interim Authorization to Operate - IATO**
  - Issued by CIO when CAT I weaknesses exist
  - IATO must be accompanied by Plan of Actions and Milestones (POA&M)
  - Intended to manage IA security weaknesses
- **Denial of Authorization to Operate – DATO**
  - Remains in effect until all corrective actions identified in the POA&M are implemented

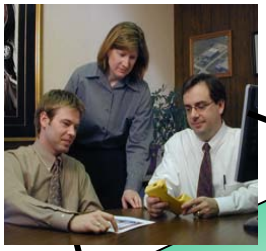
Risk Assessment Methodology

Aggregating Individual Issue Risk to Type, Site, Element Risks

Process is standardized across MDA Mission, Test, and GENSER networks

Technical Interchange Meetings (TIMs)

- C&A Team
- Government
- Developer
- Warfighter



Single Type or Site Issue Risks

Multiple Issue Risks Aggregated to Type or Site Risk

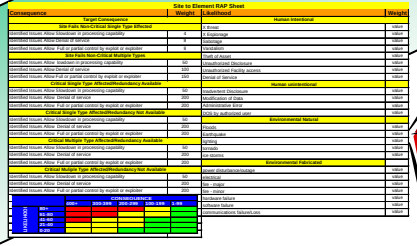
Type & Site Risks Aggregated to GMD Element Risk

GMD Element SSAA and Risk Assessment

Type X to Element Y to BMDS RAP Sheet

Consequence	Weight	Likelihood	Weight
Type X Criticality vis-à-vis Element Y		Imported Risk Rating from Type X	
Low		Type Carries a Low Risk Rating	15
Low With Redundancy	100	Type Carries a Medium Risk Rating	25
Low Without Redundancy	150	Type Carries a High Risk Rating	45
Medium			
Medium With Redundancy	150	Intelligence Factors	
Medium Without Redundancy	200	No Known Information suggesting a targeted exploit	0
High		Known Information suggests potential of a targeted exploit	25
High With Redundancy	200		
High Without Redundancy	250	Site Factors	
Functionality of Type X		No known Information at Site Hosting Type X impacts Risk	0
Role is contained within the Element	5	Known Information Exists at Site Hosting Type X: Import Site RAP Value	25
Role is critical to BMDS Interconnectivity / Communication	250		
Element Y Weighting Within BMDS			
Boost	199		
Midcourse	299		
Terminal	99		
Element Role is critical to BMDS Interconnectivity	299		

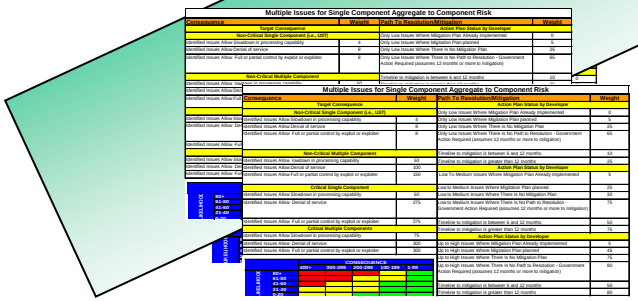
LIKELIHOOD	CONSEQUENCE 400+	300-399	200-299	100-199	1-99
80+					
61-80					
41-60					
21-40					
0-20					



Site to Element RAP Sheet

Consequence	Weight	Likelihood	Weight
Target Consequence		Human Intentional	
Site Fails Non-Critical Single Type Effected		A Asset	Value
Identified Issues: Allow Slowdown in processing capability	4	A Espionage	Value
Identified Issues: Allow denial of service	4	Corruption	Value
Identified Issues: Allow Full or partial control by exploit or exploiter	8	Vandalism	Value
Site Fails Non-Critical Multiple Types		Theft of Asset	Value
Identified Issues: Allow slowdown in processing capability	50	Unauthorized Disclosure	Value
Identified Issues: Allow Denial of service	100	Unauthorized Facility Access	Value
Identified Issues: Allow Full or partial control by exploit or exploiter	150	Denial of Service	Value
Critical Single Type Effected/Redundancy Available		Human unintentional	
Identified Issues: Allow Slowdown in processing capability	50	Inadvertent Disclosure	Value
Identified Issues: Allow Denial of service	200	Modification of Data	Value
Identified Issues: Allow Full or partial control by exploit or exploiter	250	Administrative Error	Value
Critical Single Type Effected/Redundancy Not Available		Acts by authorized user	Value
Identified Issues: Allow Slowdown in processing capability	50	Environmental Natural	
Identified Issues: Allow Denial of service	200	Floods	Value
Identified Issues: Allow Full or partial control by exploit or exploiter	250	Earthquake	Value
Critical Multiple Type Effected/Redundancy Available		Lightning	Value
Identified Issues: Allow Slowdown in processing capability	50	Tornado	Value
Identified Issues: Allow Denial of service	200	Fire Events	Value
Identified Issues: Allow Full or partial control by exploit or exploiter	250	Environmental Fabricated	
Critical Multiple Type Effected/Redundancy Not Available		Power Interruptions/Outages	Value
Identified Issues: Allow Slowdown in processing capability	50	Gas Spills	Value
Identified Issues: Allow Denial of service	200	Gas - major	Value
Identified Issues: Allow Full or partial control by exploit or exploiter	250	Gas - minor	Value
		Hardware failure	Value
		Software failure	Value
		Communications failures/Loss	Value

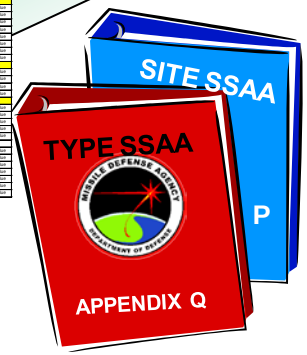
LIKELIHOOD	CONSEQUENCE 400+	300-399	200-299	100-199	1-99
80+					
61-80					
41-60					
21-40					
0-20					



Multiple Issues for Single Component Aggregate to Component Risk

Consequence	Weight	Path To Resolution/Mitigation	Weight
Target Consequence		Action Plan Status by Developer	
Non-Critical Single Component (i.e., UUT)		Only Low Issues Where Mitigation Plan Already Implemented	0
Identified Issues: Allow Slowdown in processing capability	4	Only Low Issues Where Mitigation Plan planned	5
Identified Issues: Allow Denial of service	8	Only Low Issues Where There Is No Mitigation Plan	25
Identified Issues: Allow Full or partial control by exploit or exploiter	8	Only Low Issues Where There Is No Path to Resolution - Government Action Required (assumes 12 months or more to mitigation)	65
Non-Critical Multiple Component		Timeline to mitigation is between 6 and 12 months	10
Identified Issues: Allow Slowdown in processing capability	50	Timeline to mitigation is greater than 12 months	25
Identified Issues: Allow Denial of service	100	Action Plan Status by Developer	
Identified Issues: Allow Full or partial control by exploit or exploiter	150	Low To Medium Issues Where Mitigation Plan Already Implemented	5
Critical Single Component		Low to Medium Issues Where Mitigation Plan planned	25
Identified Issues: Allow Slowdown in processing capability	50	Low to Medium Issues Where There Is No Mitigation Plan	40
Identified Issues: Allow Denial of service	275	Low to Medium Issues Where There Is No Path to Resolution - Government Action Required (assumes 12 months or more to mitigation)	75
Identified Issues: Allow Full or partial control by exploit or exploiter	275	Timeline to mitigation is between 6 and 12 months	50
Critical Multiple Components		Timeline to mitigation is greater than 12 months	75
Identified Issues: Allow Slowdown in processing capability	75	Action Plan Status by Developer	
Identified Issues: Allow Denial of service	300	Up to High Issues, Where Mitigation Plan Already Implemented	5
Identified Issues: Allow Full or partial control by exploit or exploiter	300	Up to High Issues, Where Mitigation Plan planned	45
		Up to High Issues, Where There Is No Mitigation Plan	75
		Up to High Issues, Where There Is No Path to Resolution - Government Action Required (assumes 12 months or more to mitigation)	95
		Timeline to mitigation is between 6 and 12 months	50
		Timeline to mitigation is greater than 12 months	95

SEVERITY	CONSEQUENCE 400+	300-399	200-299	100-199	1-99
80+					
61-80					
41-60					
21-40					
0-20					



GMD Type & Site Test Results and Risk Assessments