IDA

A Security Risk Management Response To Emerging Threats

2011 GEOINT Protection Conference
November 16, 2011

Bruce Low
Research Staff Member
Institute for Defense Analyses
hlow@IDA.org

Response of the Technology Protection Community to Emerging Threats

- The Technology Protection Planner's Environment
  - Traditional Security Planning
  - Improved Risk Avoidance Model
  - Security Risk Management Advanced Methodology Demonstrator (AMD)
- All Risk Management Planning is Threat Driven
  - What Threat Information Does the Protection Planner Need to Plan How to Mitigate Security Risks to Technologies and Programs?

IDA | Traditional Security Planning

- Establish the Compliance Security Baseline
  - Personnel Security
  - Information Security (including Cyber Security)
  - Physical Security
  - Technical Security
  - Security Training and Awareness

IDA | Improved Risk Avoidance

- Establish the Compliance Security Baseline
  - Personnel Security
  - Information Security (including Cyber Security)
  - Physical Security
  - Technical Security
  - Security Training and Awareness
- Develop List of Designated Science and Technology Information (DS&TI) and Critical Program Information (CPI) for Focused Protection Activities

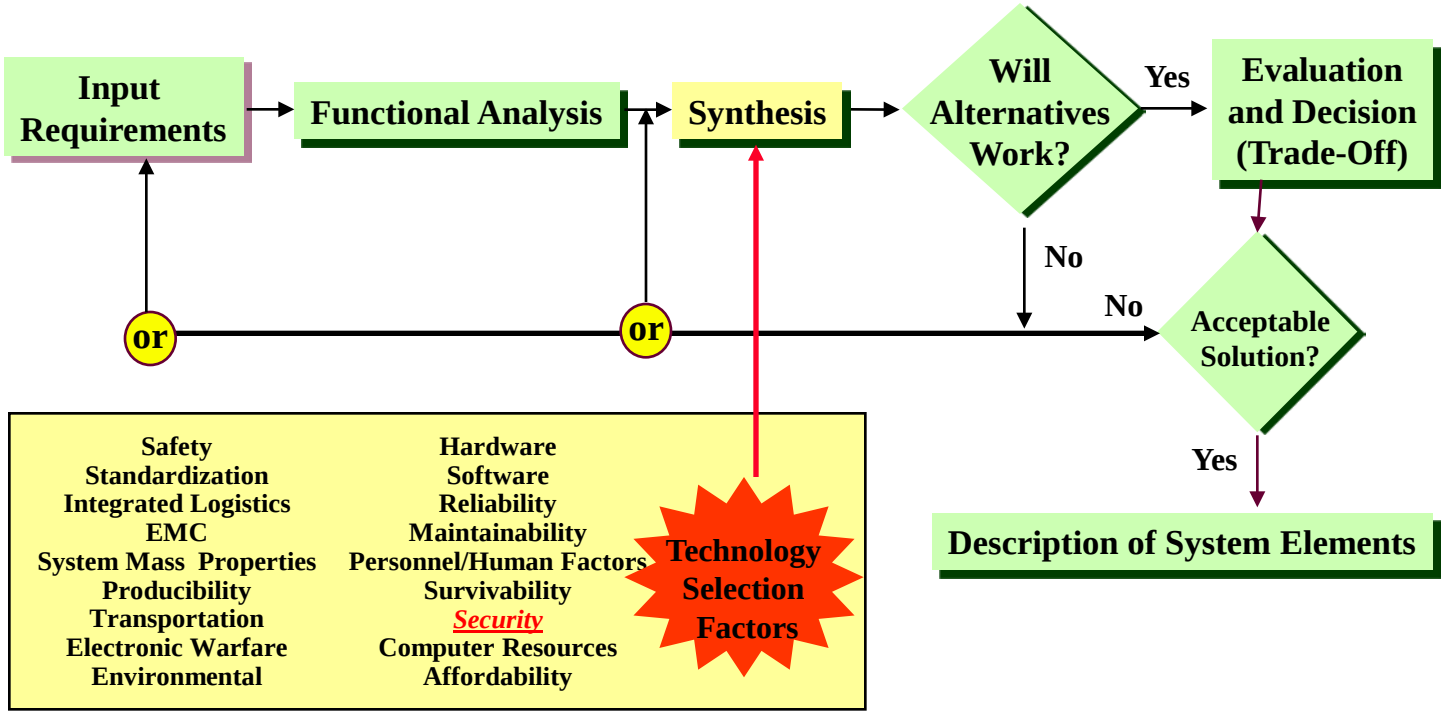
Security Risk Management Protection Advanced Methodology Model

- Establish the Compliance Security Baseline
  - Personnel Security
  - Information Security (including Cyber Security)
  - Physical Security
  - Technical Security
  - Security Training and Awareness
- Develop List of Designated Science and Technology Information (DS&TI) and Critical Program Information (CPI) for Focused Protection Activities
- Builds on Solid Foundation of Compliance-Based Countermeasures and DS&TI/CPI Focus
  - Performs Impact of Loss Assessment
  - Assesses Multi-Disciplinary Counterintelligence Threats, Export Control Issues and Horizontal Protection Equities to Both Technologies and Programmatics
  - Recommends Protection Strategy *Based On Assessed Threats*
  - Recommends Most Cost Effective Combination of Risk Mitigation Protection Activities

IDA | Origins of the Security Risk Management AMD

Based on Systems Engineering Model

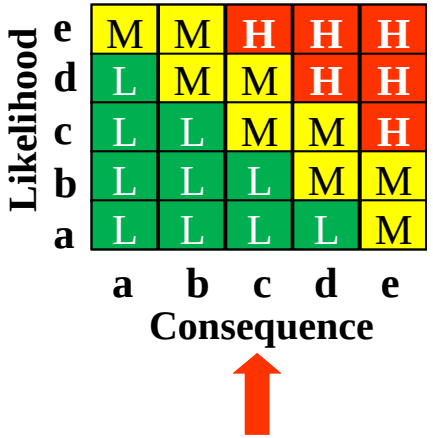
Systems Security Engineering



IDA | Introduced Risk Cube and Metrics

Level	What Is The Likelihood the Risk Event Will Happen?
a	Remote
b	Unlikely
c	Likely
d	Highly Likely
e	Near Certainty

Process Variance refers to deviation from best practices. Likelihood/Probability refers to risk events.



Risk Assessment

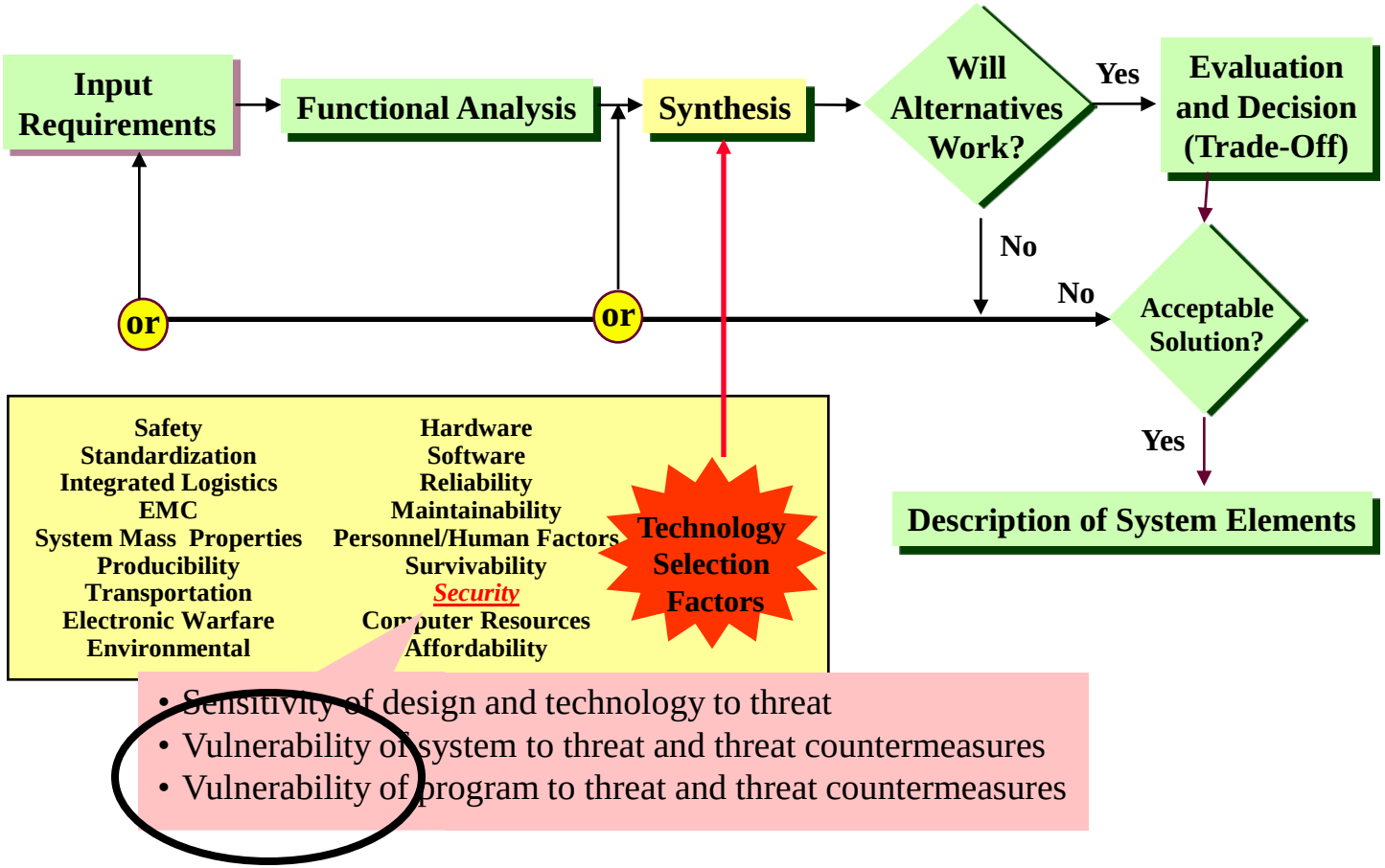
R/H	HIGH – Unacceptable. Major disruption likely. Different approach required. Priority management attention required.
Y/M	MODERATE – Some disruption. Different approach may be required. Additional management attention may be needed.
G/L	LOW – Minimum impact. Minimum oversight needed to ensure risk remains low.

Cost
Schedule
Performance

Level	Technical Performance	and/ or	Schedule	and/ or	Cost	and/ or	Impact on Other Teams
a	Minimal or no impact		Minimal or no impact		Minimal or no impact		None
b	Acceptable with some reduction in margin		Additional resources required; able to meet need dates		<5%		Some impact
	Acceptable with significant reduction in margin		Minor slip in key milestones; not able to meet need date		5 -7%		Moderate impact
d	Acceptable; no remaining margin		Major slip in key milestone o r critical path impacted		7-10%		Major impact
e	Unacceptable		Can't achieve key team or major program milestone		>10%		Unacceptable

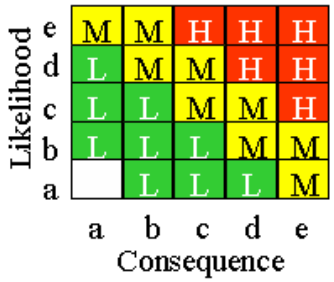
‘Vulnerability’ of Technology and Program Are Key Metrics

Program Protection Engineering Introduced



IDA | Defined the New Metric

Level	Vulnerability
a	No data on which to base an analysis
b	Unlikely data will be collected
c	Less than even chance data will be collected and accurately analyzed
d	Data might be collected and accurately analyzed
e	Highly probable data will be collected and accurately analyzed



Level	Countermeasures Effectiveness
	No data on which to base an analysis
	Multiple layers of effective countermeasures exist.
	The majority of countermeasures in place are effective, however some peripheral susceptibilities to successful collection and analysis remain.
	There are some effective countermeasures in place, but significant unmitigated susceptibilities to successful collection and analysis remain.
e	There are no countermeasures in place to mitigate collection and analysis threat

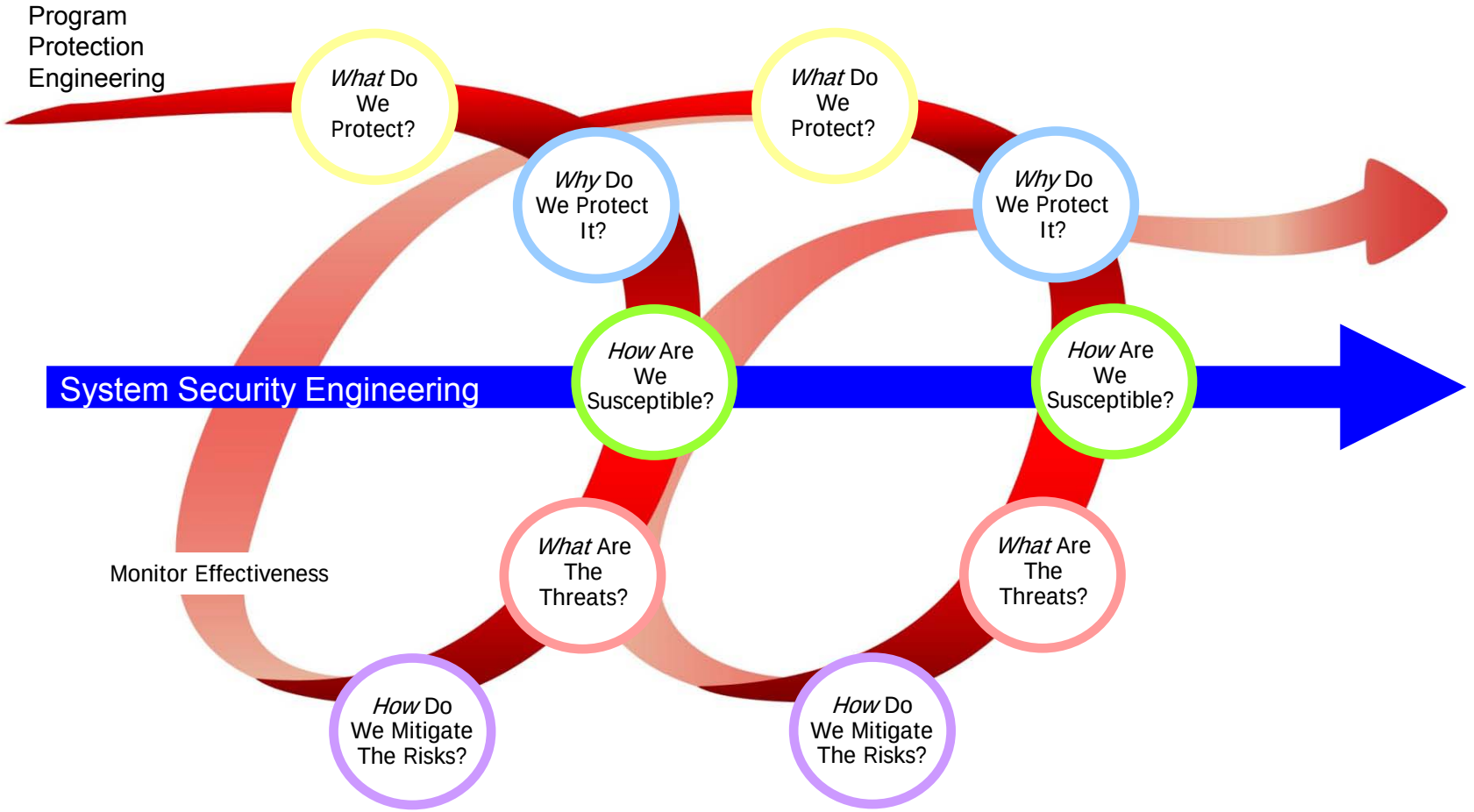
Residual Risk Assessment

G/L	Multiple layers of effective countermeasures exist. Few or no known adversaries would be capable of exploiting this system.
Y/M	Inconsistencies of countermeasures in place leave multiple susceptibilities through which adversaries might be capable of exploiting compromises concerning this mission critical or mission essential system.
R/H	Lack of effective countermeasures to collection and successful analysis of CPI will allow known adversaries to exploit compromises of this mission critical system.

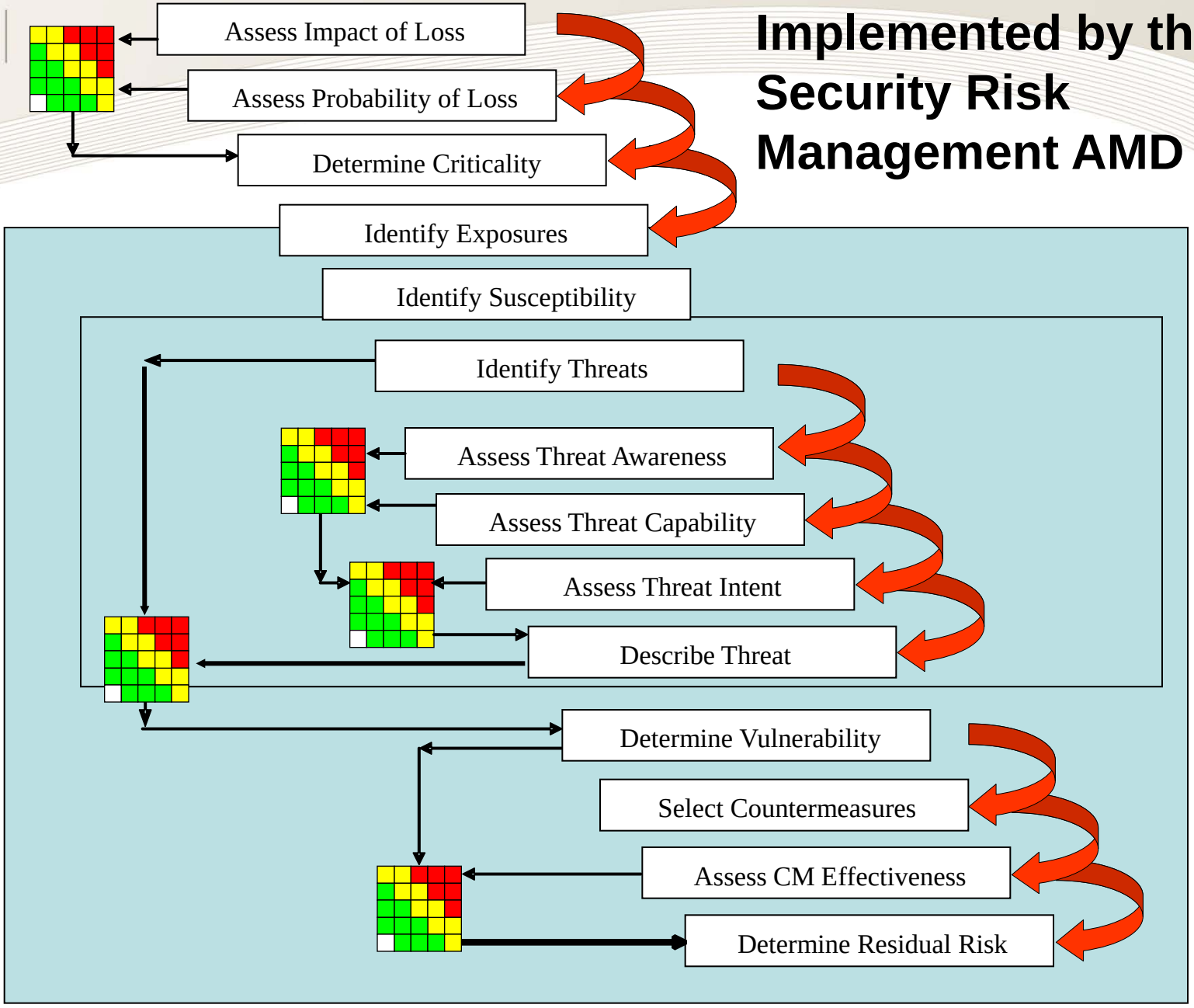
Cost
Schedule
Performance
Security

IDA | Unifying Strategy Covers Full Life Cycle

What do we protect? *Why* do we protect it? *How* are we susceptible? *What* are the threats? *How* do we mitigate the risks?

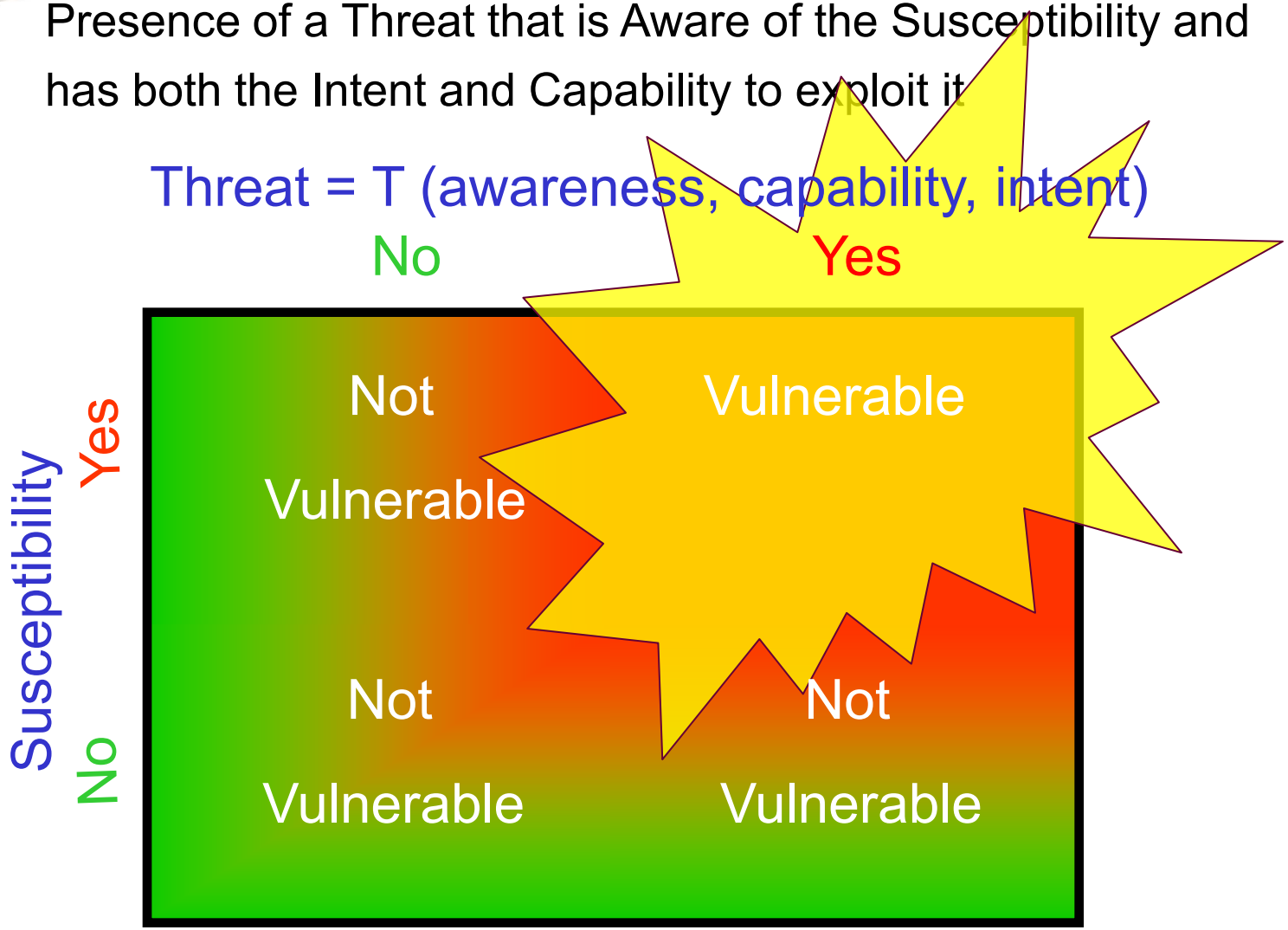


Implemented by the Security Risk Management AMD



Accurate Threat Data is Critical Input to Methodology

- In its simplest form a Vulnerability is a Susceptibility in the Presence of a Threat that is Aware of the Susceptibility and has both the Intent and Capability to exploit it



IDA | What Threat Data Do We Need?

AWARENESS?

HOW MUCH DOES THE THREAT KNOW ABOUT THE PROGRAM?

- FUNDING
- KEY STAFF
- PRIORITY

HOW MUCH DOES THE THREAT KNOW ABOUT THE TECHNOLOGY?

- CRITICALITY
- MISSION AREA

INTENT?

- WILLING TO RISK ASSETS?
- EXPOSE SOURCES AND METHODS?

THREAT ASSESSMENT

Capability to Collect and Exploit?

- Collect critical *program* information?
- Collect critical *technology* information
- Understand and apply the information against U.S. or allies?

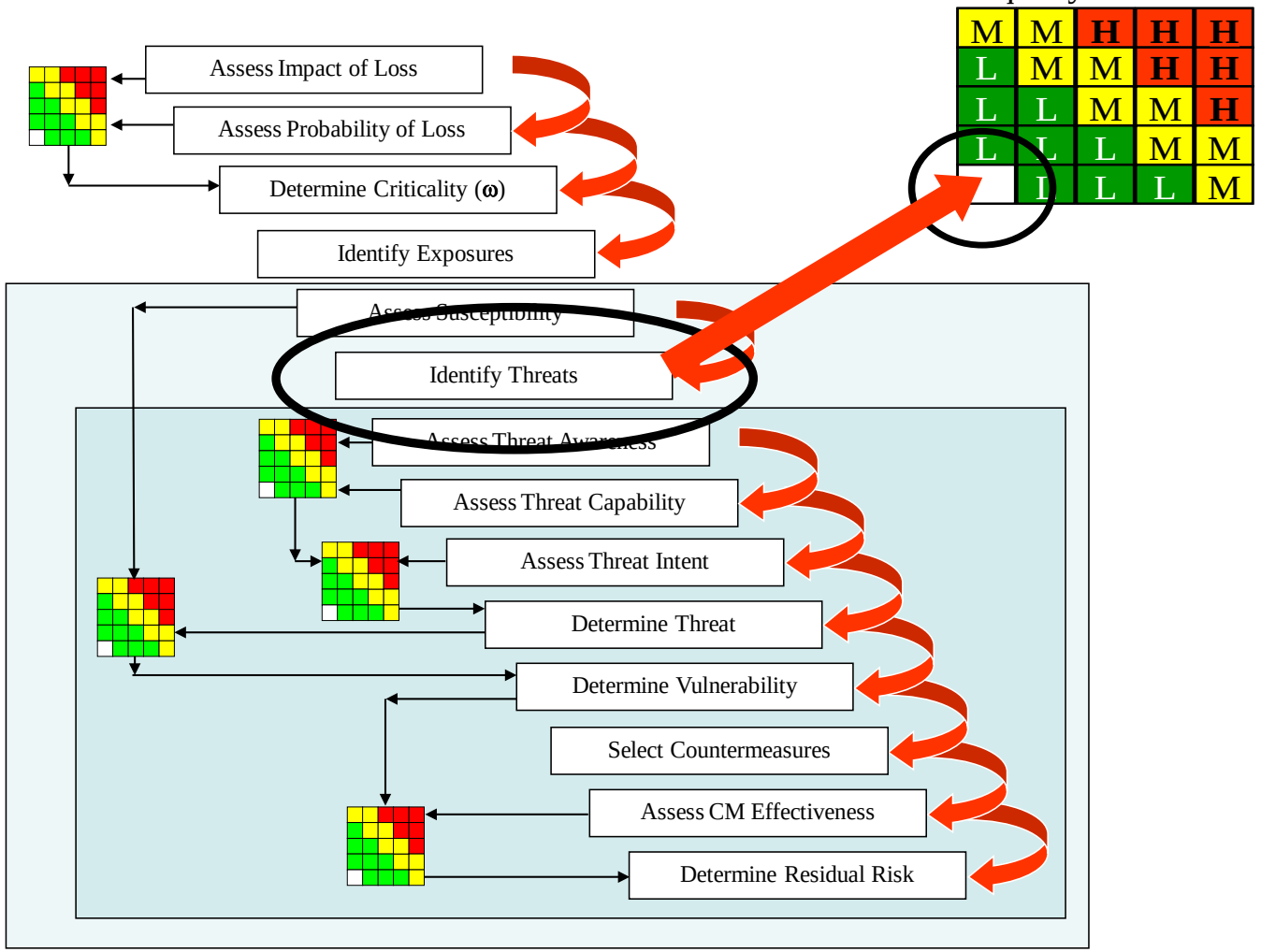
IDA | The Intensity of the Threat is a Critical Input

- To Determine the 'Vulnerability' of Program and Technology Information to Collection, Analysis and Exploitation, We Assess the Information 's 'Susceptibility' to Collection (Described as S_{Low} – $S_{Critical}$), Operating in the Presence of a Collection and Exploitation Threat.
  - The Threat is Comprised of an Adversary that is *Aware* of the Existence of the Technology ($T_{Low\ Awareness}$ – $T_{Critical\ Awareness}$), and has Both *Capability* to Exploit the Susceptibility to Collection ($T_{Low\ Capability}$ – $T_{Critical\ Capability}$), and the *Intent* to Collect and Analyze the Information ($T_{Low\ Intent}$ – $T_{Critical\ Intent}$)
  - The Combination of 'S' and 'T' Factors are the Program's or Technology's 'Vulnerability' (V_{Low} – $V_{Critical}$)

IDA | Traditional Threat Factors in Security Risk

Getting Credible and Timely Threat Data is Critical

Risk Avoidance - Threat is Unknown; All Classified and Sensitive Data is Protected Equally



Information Quality Matters!

- **Specific Threat** – Threat is Well Defined and Accurately Characterized – *The Ideal but Least Likely*
  - Who is Collecting Against My Program?
  - Who is Collecting Against My Technology?
  - Who is Collecting Against My Organization?
- **Informed Threat** – Threat is Unknown, but Generic Threat Data for Most Likely Actor(s) Available – *the Most Likely Norm*
- **Improved Risk Avoidance** – Threat is Unknown; Threat Data for Worst Case Actor Normal Collection Methods Used; Countermeasures are Prioritized Based on Criticality Assessments – *the Current State*

IDA | Information Quality Matters!

- **Specific Threat** – Threat is Well Defined and Accurately Characterized – *The Ideal but Least Likely*
  - Who is Collecting Against My Program?
  - Who is Collecting Against My Technology?
  - Who is Collecting Against My Organization?
- **Informed Threat** – Threat is Unknown, but Generic Threat Data for Most Likely Actor(s) Available – *the Most Likely Norm*
- **Improved Risk Avoidance** – Threat is Unknown; Threat Data for Worst Case Actor Normal Collection Methods Used; Countermeasures are Prioritized Based on Criticality Assessments – *the Current State*

IDA | Information Quality Matters!

- **Specific Threat** – Threat is Well Defined and Accurately Characterized – *The Ideal but Least Likely*
  - Who is Collecting Against My Program?
  - Who is Collecting Against My Technology?
  - Who is Collecting Against My Organization?
- **Informed Threat** – Threat is Unknown, but Generic Threat Data for Most Likely Actor(s) Available – *the Most Likely Norm*
- **Improved Risk Avoidance** – Threat is Unknown; Threat Data for Worst Case Actor Normal Collection Methods Used; Countermeasures are Prioritized Based on Criticality Assessments – *the Current State*

IDA | Information Quality Matters!

- **Specific Threat** – Threat is Well Defined and Accurately Characterized – *The Ideal but Least Likely*
  - Who is Collecting Against My Program?
  - Who is Collecting Against My Technology?
  - Who is Collecting Against My Organization?
- **Informed Threat** – Threat is Unknown, but Generic Threat Data for Most Likely Actor(s) Available – *the Most Likely Norm*
- **Improved Risk Avoidance** – Threat is Unknown; Threat Data for Worst Case Actor Normal Collection Methods Used; Countermeasures are Prioritized Based on Criticality Assessments – *The Current State*
- **Absolute Risk Avoidance** - Threat is Unknown; All Classified and Sensitive Data is Protected Equally –*Unacceptable*

IDA | Impact of Emerging Threats TBD

Virtual Communities

Crowd-Sourcing

Social Media

Robot Apprenticing

Ubiquitous Digital Exhaust

Collective Intelligence

Living in Exponential Times

Identity Theft

Homomorphic Encryption

Revolution in Sensemaking

Social Networking

Re-humanized Online Collaboration

New Organizational Models

Apps

Additive Manufacturing

REDEFINITION OF SCALE

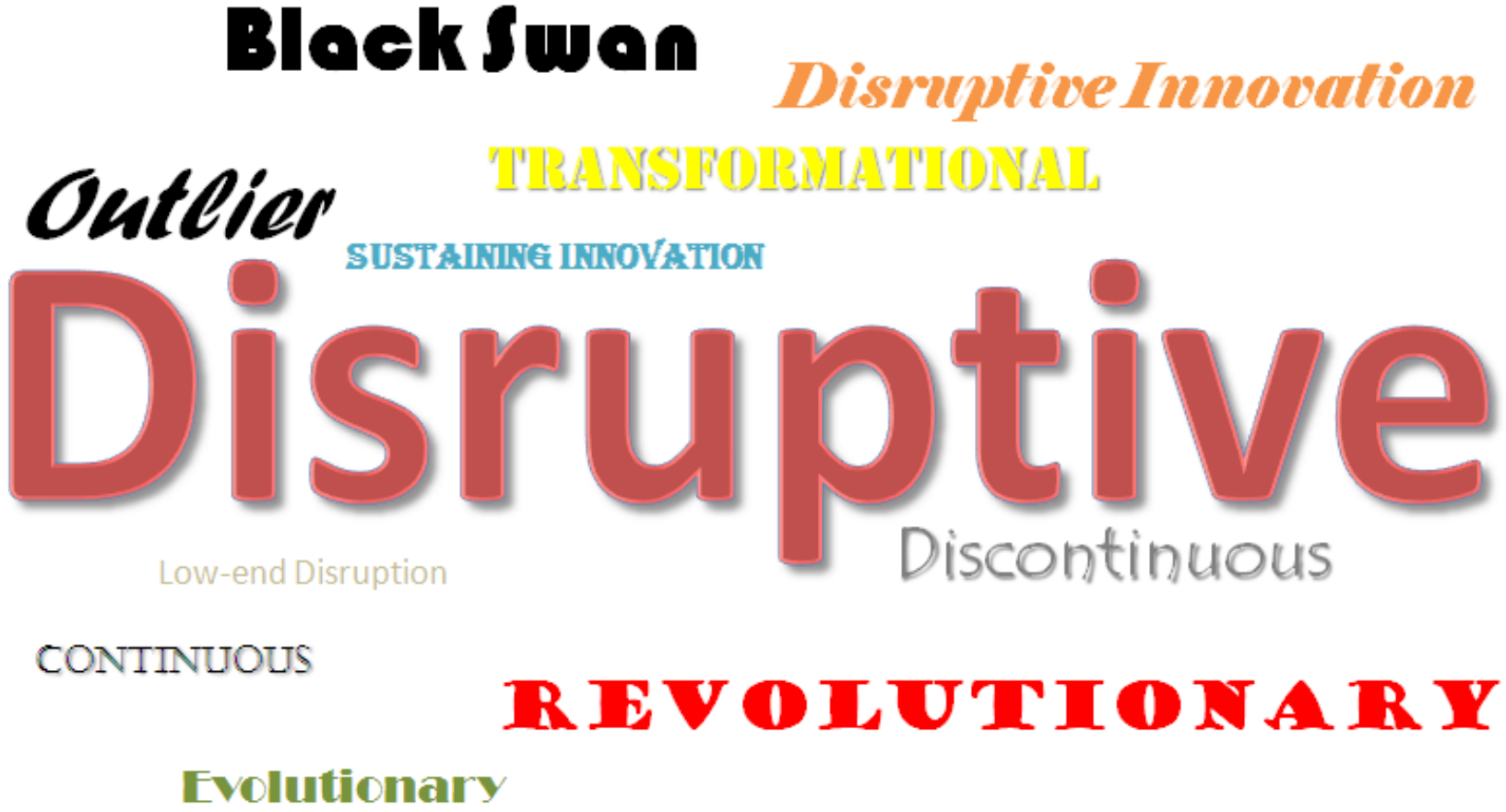
Cloud Computing

Biometric Matching

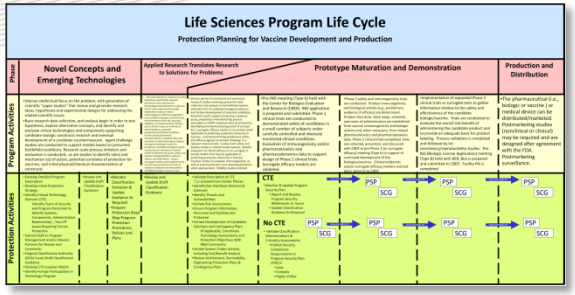
Ubiquitous Computing

IDA | What is the Impact of Emerging Threats on this Model?

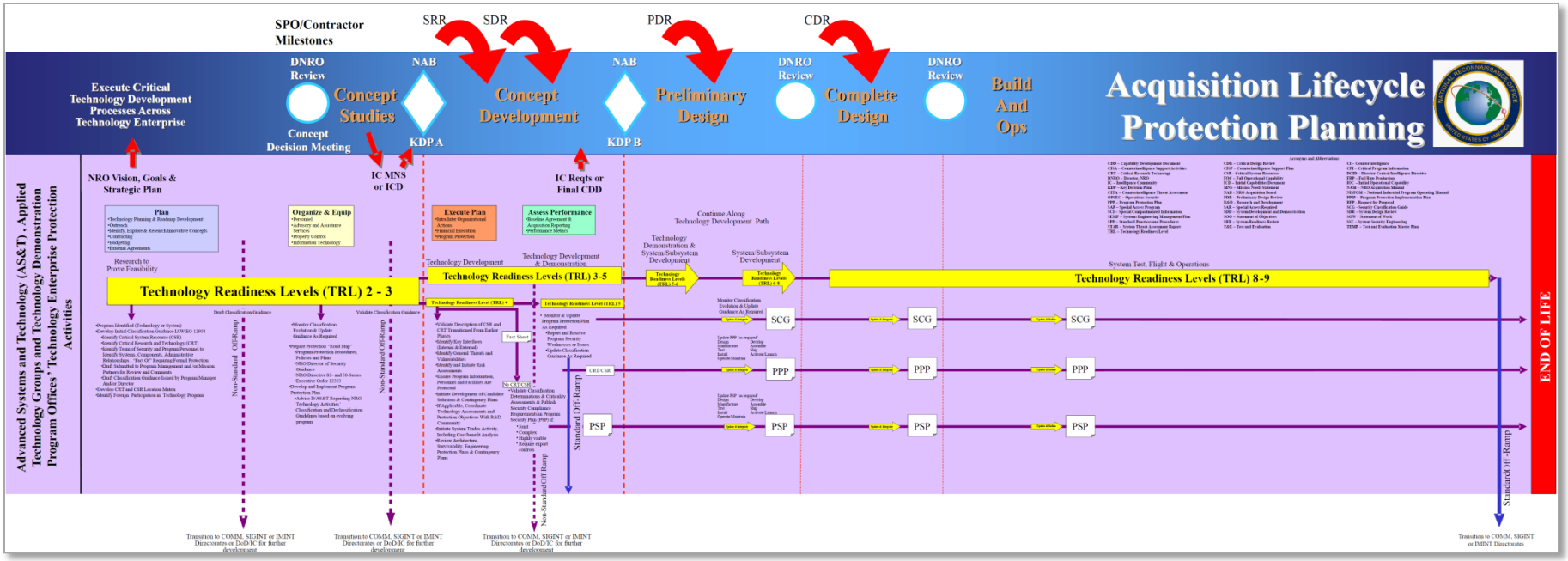
- Definition of New Threat and Degree of Change



IDA | R&D Sponsorship is 2nd Most Important Factor



- Culture of Participants
- Infrastructure's Experience Dealing With Full Spectrum of Threats
- Complexity of Tasks



How are we doing?

What Do We Protect? *Why* Do We Protect It? *How* Are We Susceptible? *What* Are the Threats? *How* Do We Mitigate the Risks? These Factors Are Fully Integrated by Technology Protection and Program Protection Teams Into the *Security Risk Management* AMD To Develop And Implement Tailored Security Risk Mitigation Activities

Timely, Credible Multi-Disciplinary Threat Information is the Most Important Factor, both now and in the future, to the Success of the Security Risk Management Approach!!

Bruce Low is a Research Staff Member of the Institute for Defense Analyses, an FFRDC with Defense, Intelligence and other Executive Branch core tasks. His background includes both extensive technical intelligence collection and exploitation experience and high technology protection planning in the systems security engineering and mission assurance arenas. He can be reached at Hlow@IDA.org.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
16-11-2011	IAD Draft Final	2011

4. TITLE AND SUBTITLE

A Security Risk Management Response to Emerging Threats

5a. CONTRACT NUMBER
DASW01-04-C-0003

5b. GRANT NUMBER
— — —

5c. PROGRAM ELEMENT NUMBER
— — —

6. AUTHOR(S)

Low, Howard B.

5d. PROJECT NUMBER
— — —

5e. TASK NUMBER

5f. WORK UNIT NUMBER
— — —

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER
D-NS 4476
H11-001714

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Technology Protection Branch
National Geospatial-Intelligence Agency
NGA Campus East
7500 GEOINT Drive
Springfield, VA 22150

10. SPONSOR/MONITOR'S ACRONYM(S)
NGA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
— — —

12. DISTRIBUTION / AVAILABILITY STATEMENT
This draft final has not been approved by the sponsor for distribution and release. Reproduction or use of this material is not authorized without prior permission from the responsible IDA Division Director.

13. SUPPLEMENTARY NOTES
— — —

14. ABSTRACT

Threat community support to security risk management-based technology protection planning for sensitive and classified R&D activities within the US Government takes two basic forms: 1) description of the multidiscipline counterintelligence threat to the activity's people, technology and programmatics; and, 2) description of the system security engineering threat to the activity's technology. This presentation will describe the process for assessing and integrating information about these threats as a baseline for the discussion of adjusting to emerging threats.
Emerging threats may be 'evolutionary' developments of well-understood threats, or 'revolutionary' capabilities if they represent significant advances providing threat actors with an intelligence advantage for which there are no immediate risk mitigation responses.
The risk accruing from both classes of threats (evolutionary and revolutionary) may be minimized during R&D by the protection planner, however, by reducing the opportunities for threat actors to collect critical program data and by choosing an appropriate suite of countermeasure to mitigate the remaining risks based on a cost/benefit assessment. This presentation will describe an advanced methodology demonstrator, tested in several operational environments over the past five years, which shows promise for being able to accomplish this goal. The presentation also describes the linkage between the successes of protection planning to the quality of threat information.

15. SUBJECT TERMS
security risk management, advanced methodology demonstrator, AMD, emerging threats, security risk management methodology, risk avoidance, security planning, compliance security, designated science and technology information, DS&TI, critical program information , CPI, multi-disciplinary counterintelligence threats, multi-disciplinary counterintelligence threat assessment, MDCITA, risk mitigation, system vulnerability, program vulnerability

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Bruce H. Low
Unclassified	Unclassified	Unclassified	Unlimited	26	19b. TELEPHONE NUMBER *(include area code)* 703-845-2549