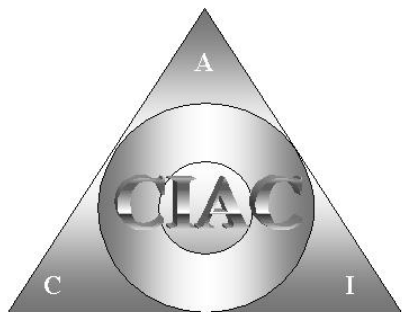


Center for Information Assurance and Cybersecurity: a PNNL and UW Collaboration

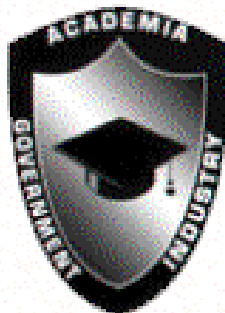
Update and Next steps



Center for Information Assurance and Cybersecurity (NSA/DHS CAE-R)



CIAC



Center for Information Assurance and Cybersecurity at the University of Washington

- **Promotes** regional, national, international collaboration
- **Produces** multi-disciplinary education and research
- **Provides** CNSS certification for students
- **Prepares** professional IA leaders efficiently



<http://ciac.ischool.washington.edu/>

Regional Leadership through Shared Strengths

Pacific Northwest National Laboratory



Advancing Science

Benefiting our Nation

New Ideas – New Generations

Advancing Science

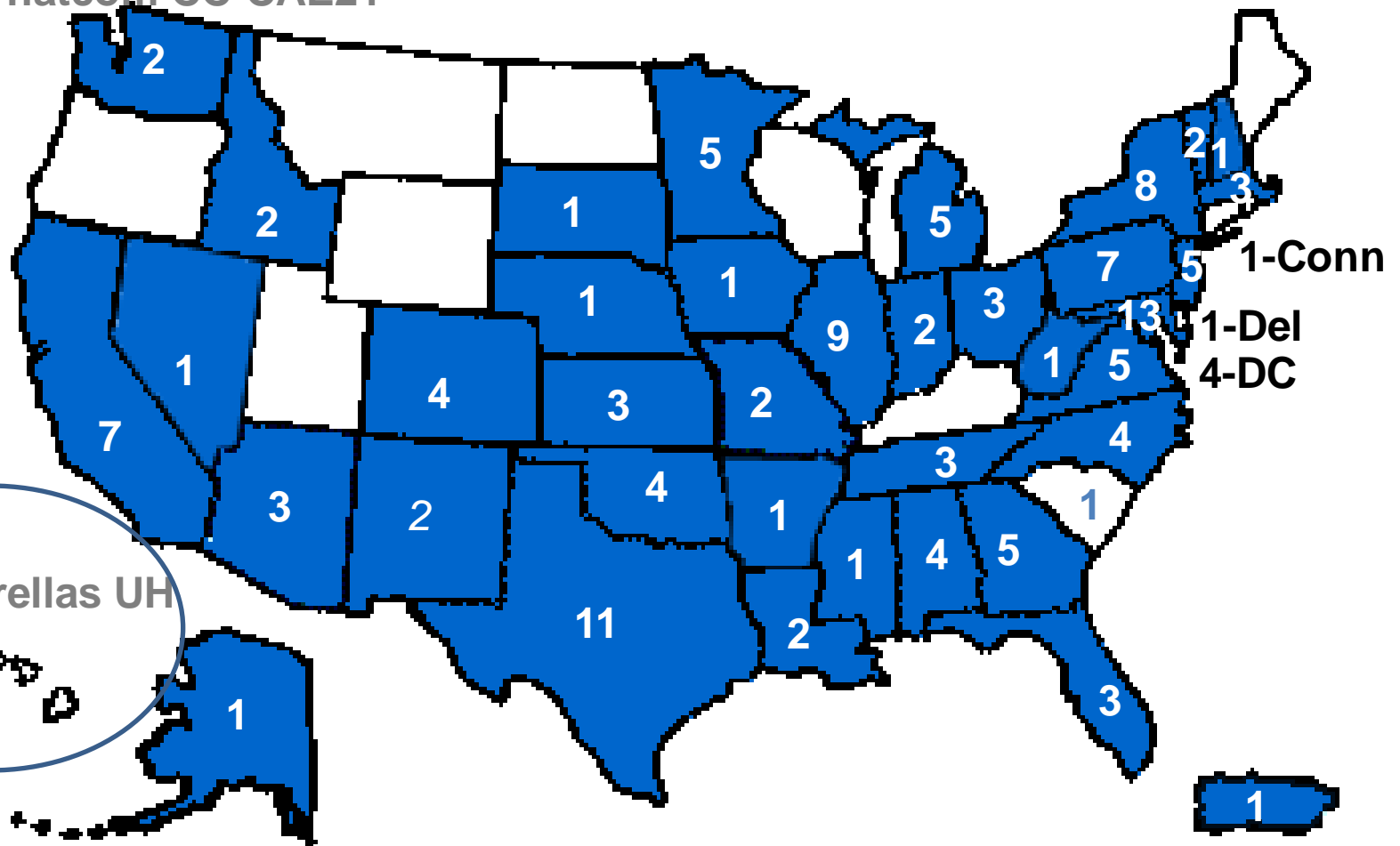


Information and Infrastructure
Integrity Initiative



CAE-IA Map 2011

2004 University of Washington CAE-R
2010 Whatcom CC-CAE2Y



UW Umbrellas UH



NSA/DHS NIETP Program

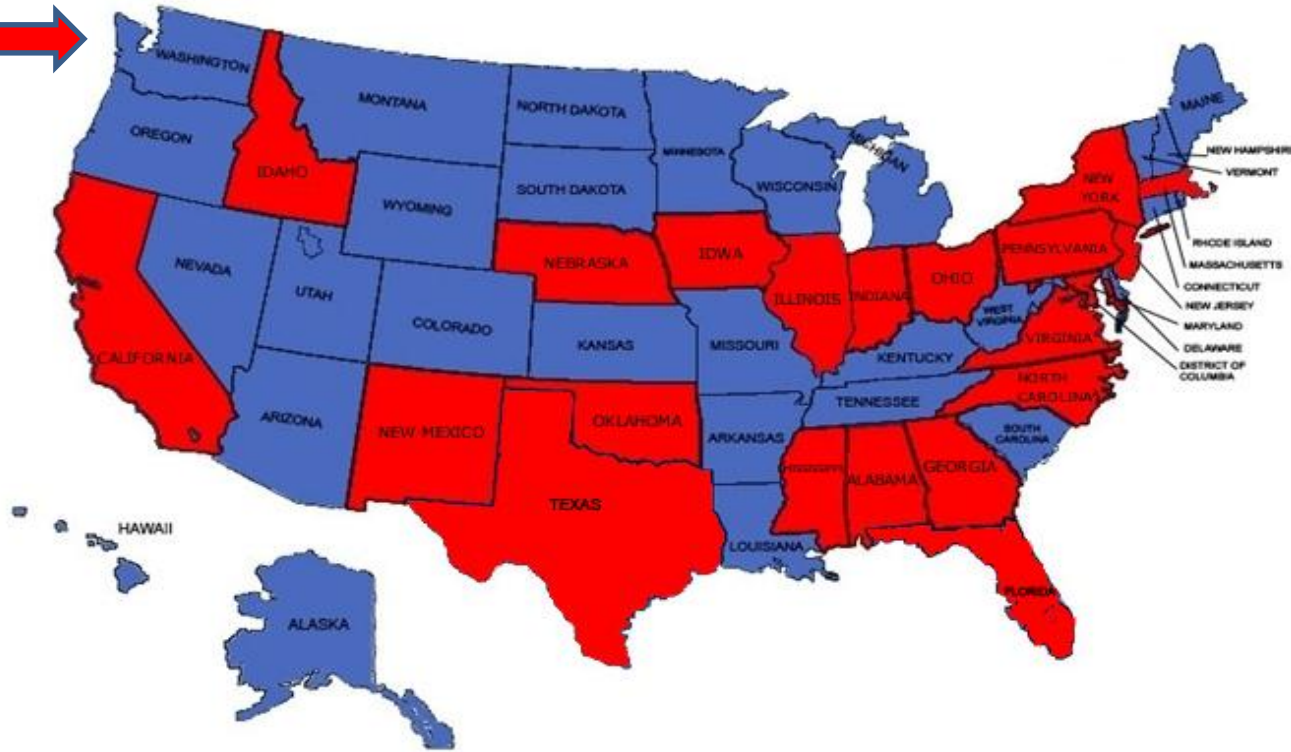
http://www.nsa.gov/ia/academic_outreach/iace_program/niaetp.shtml


- 130+ CAE's or CAE2Y's
- 30+ are CAE-R's, including:
 - UC Davis
 - Naval Post Graduate School
 - Georgia Tech
 - Johns Hopkins
 - Boston U
 - Dartmouth
 - Princeton
 - Rutgers
 - SUNY Buffalo
 - AFIT
 - Carnegie Mellon
 - Purdue
 - George Mason
 - Texas A&M
 - GWU
- 1 CAE/CAE-R in State of Washington/Hawaii

SFS Participating Institutions

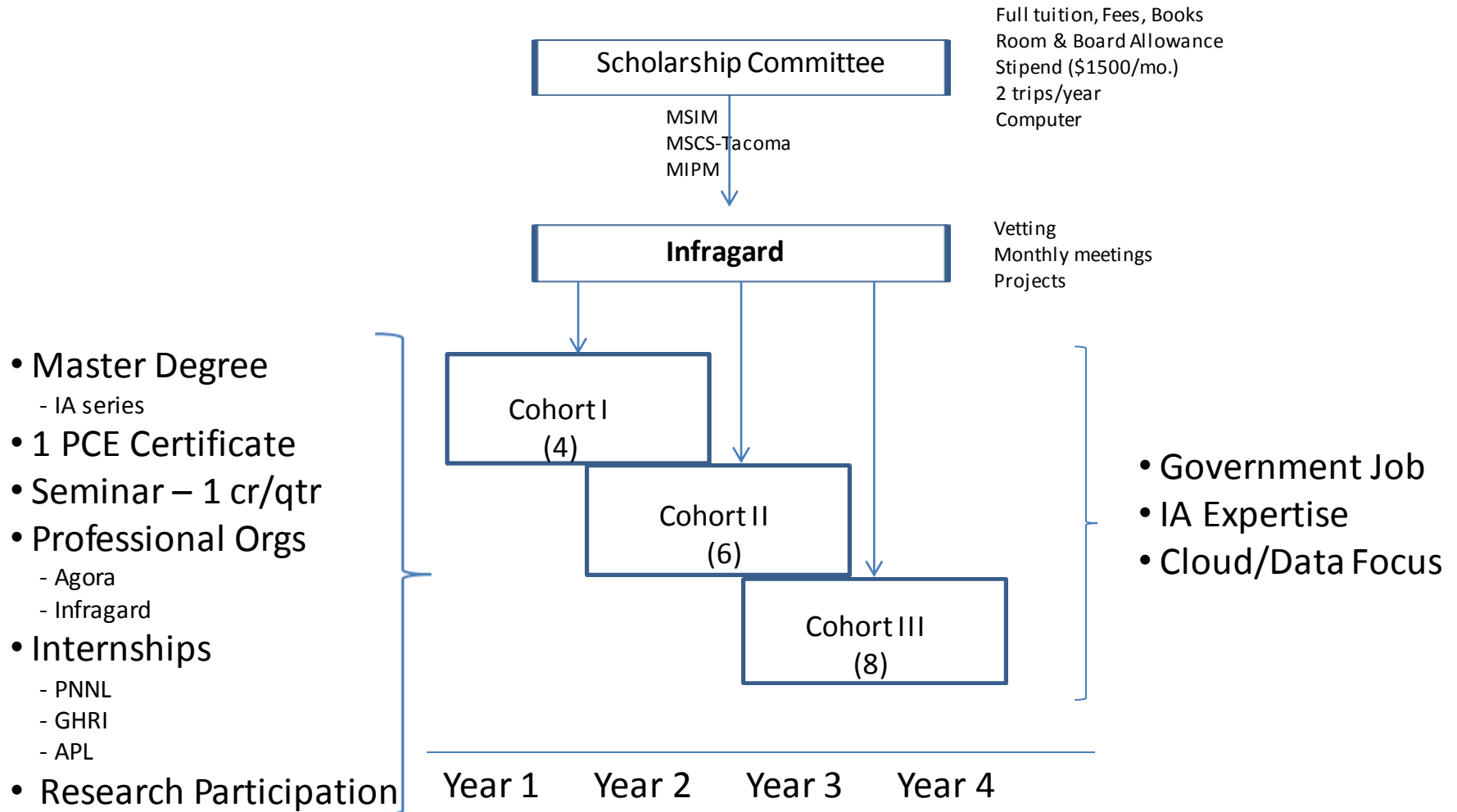
NEW!!

University of Washington



 = States with at least one school participating

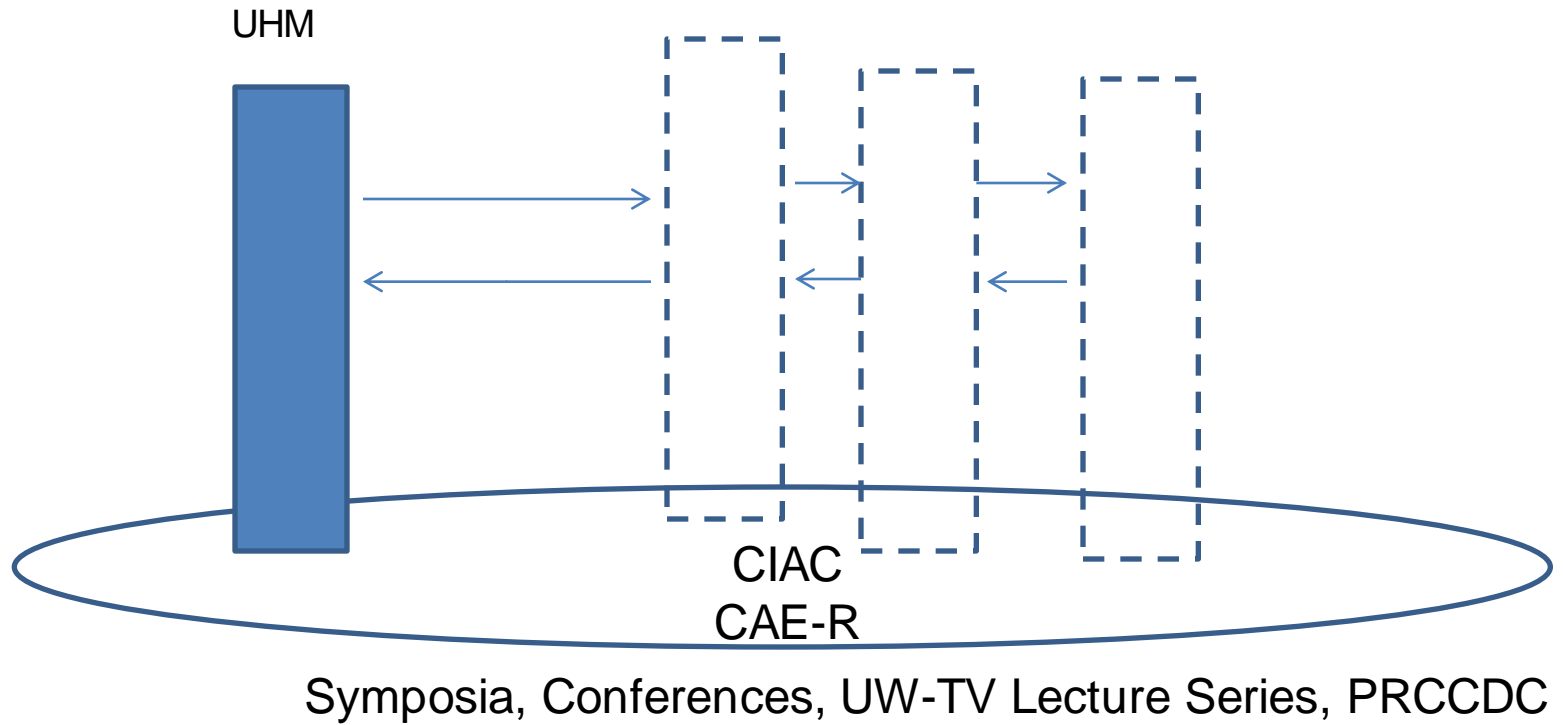
Managing Security in the Cloud: Innovative Scholarship for Service Program



Collaborative Commons

CIAC CONCEPTUAL FOUNDATION

CIAC as Collaborative Environmental Eco-System



The CIAC



International

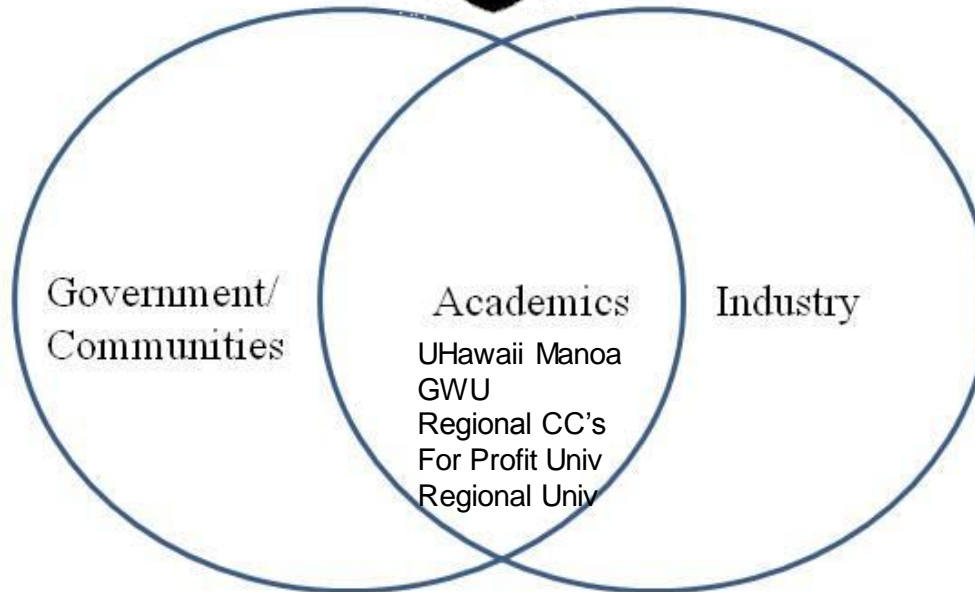
Aberystwyth, Wales
UBC, Vancouver
DGIST, S Korea

National

PNNL
NSA
DC3
GHRI-SHARP

Local

APL
PRIZM, City Light
Port of Seattle
Port of Tacoma



Public Companies

Microsoft
Amazon
Booz Allen
Boeing
TMobile

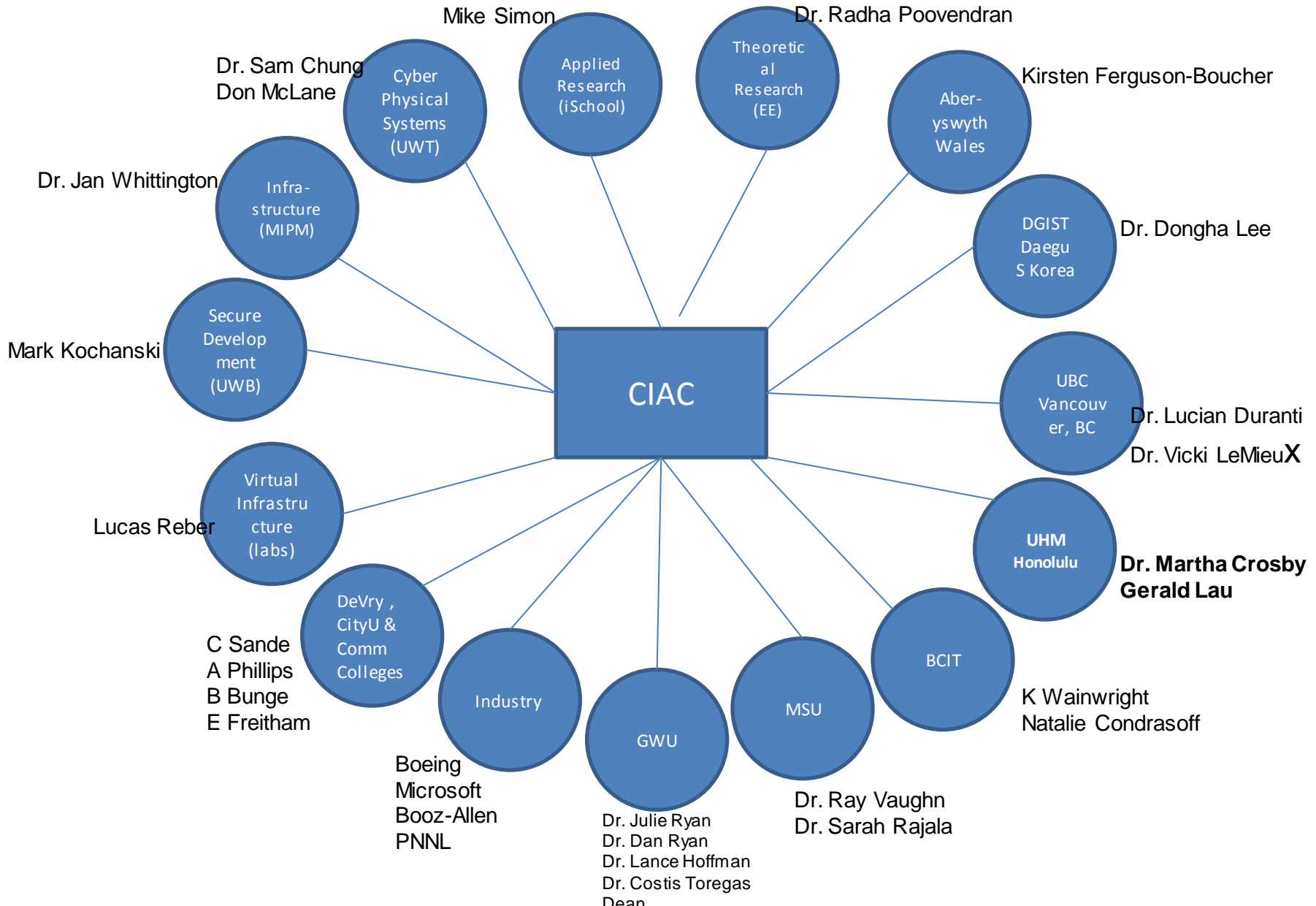
Private Companies

KPMG
DeLoitte
PW

Entrepreneurs

Creation Logic
2B3D
IO Active
Intellius
ZANTZZ

CIAC Network of Collaborators



Formal Academic Collaborations

- MOU's

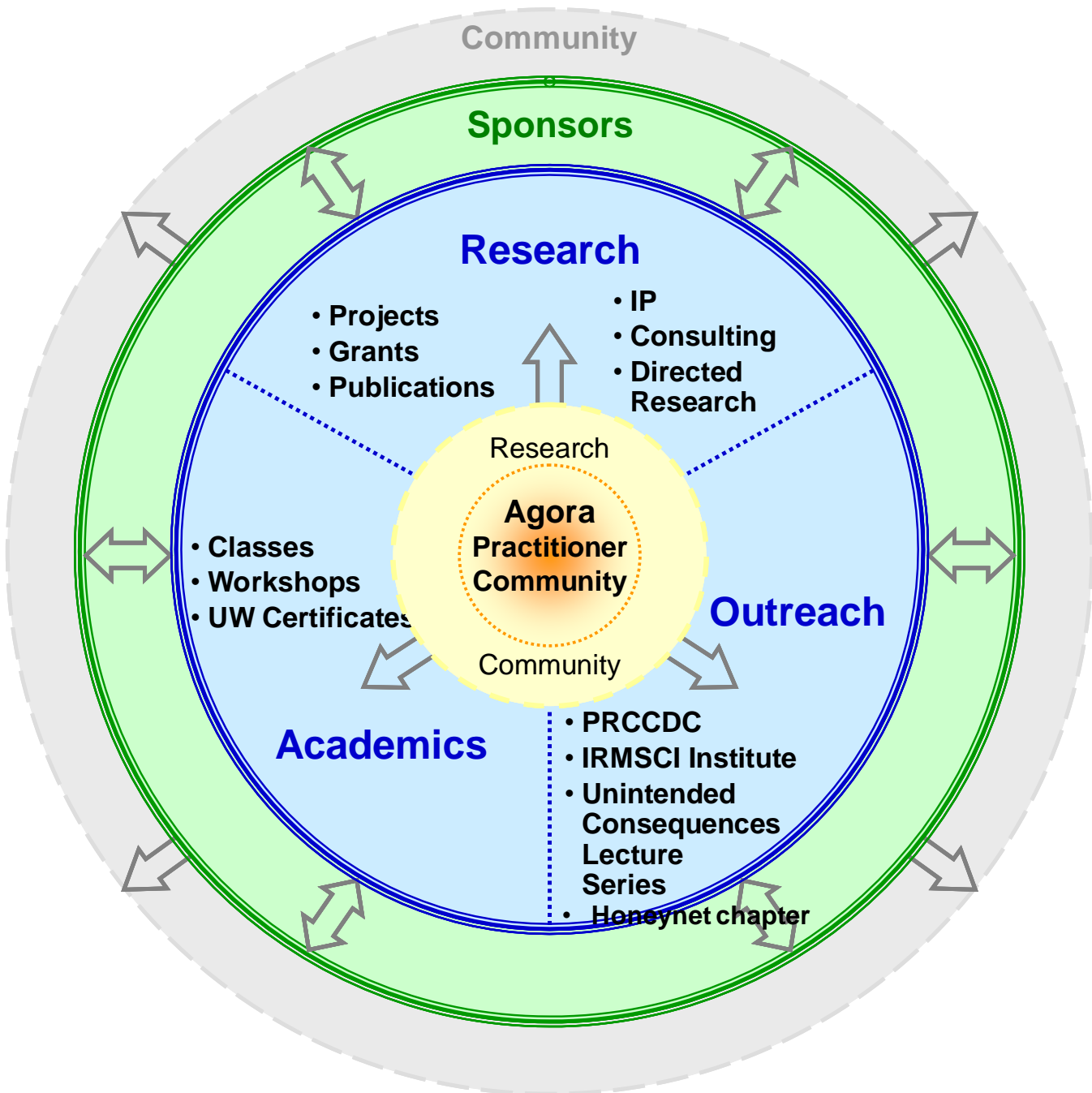
- University of Hawaii Manoa
- DGIST, Daegu South Korea
- Aberyswyth University, Wales
- University of British Columbia, Vancouver BC

- Research Co-PIs

- University of Hawaii Manoa
- George Washington University
- Mississippi State University
- British Columbia Institute of Technology



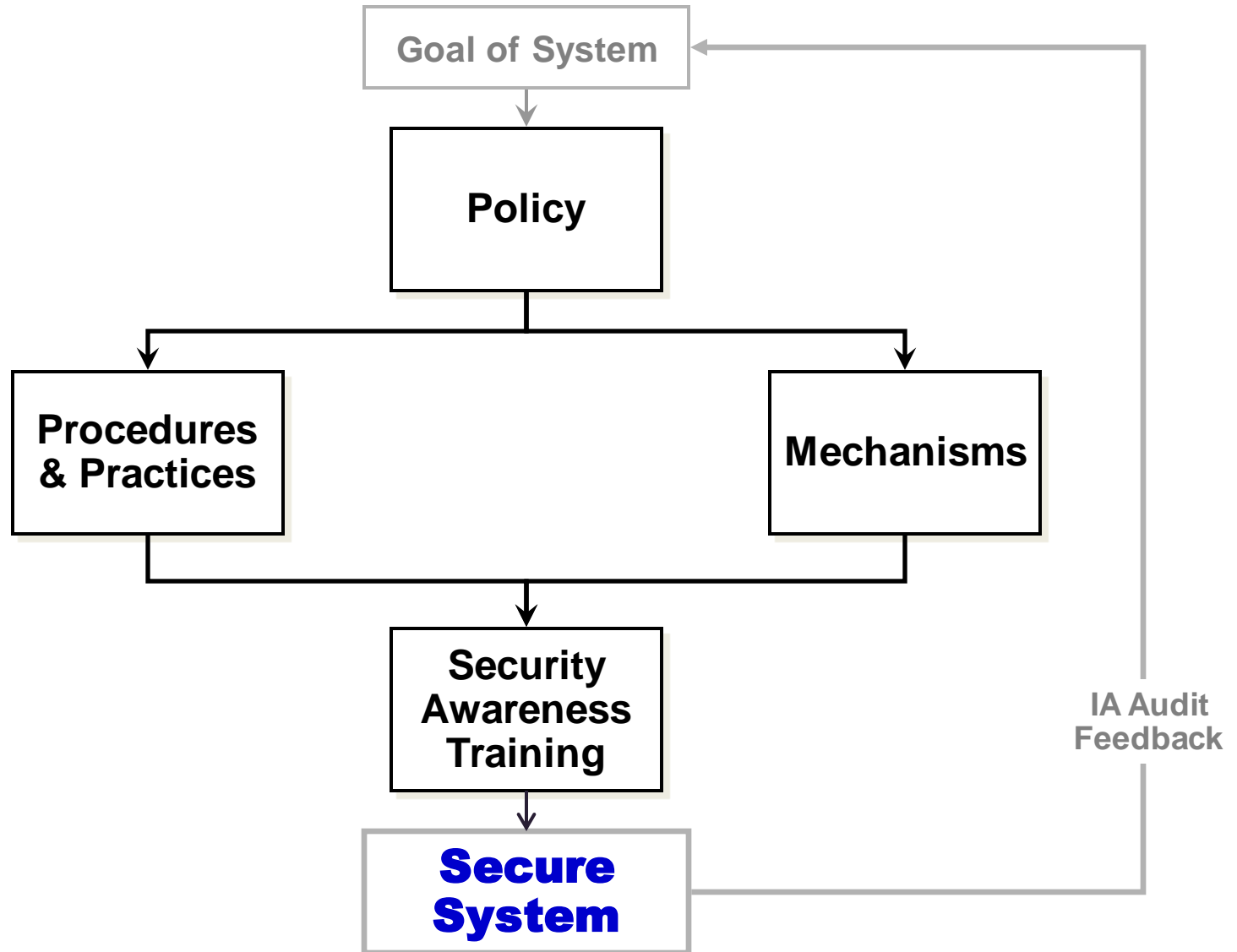
Center for Information Assurance and Cybersecurity
NSA-CAE-R



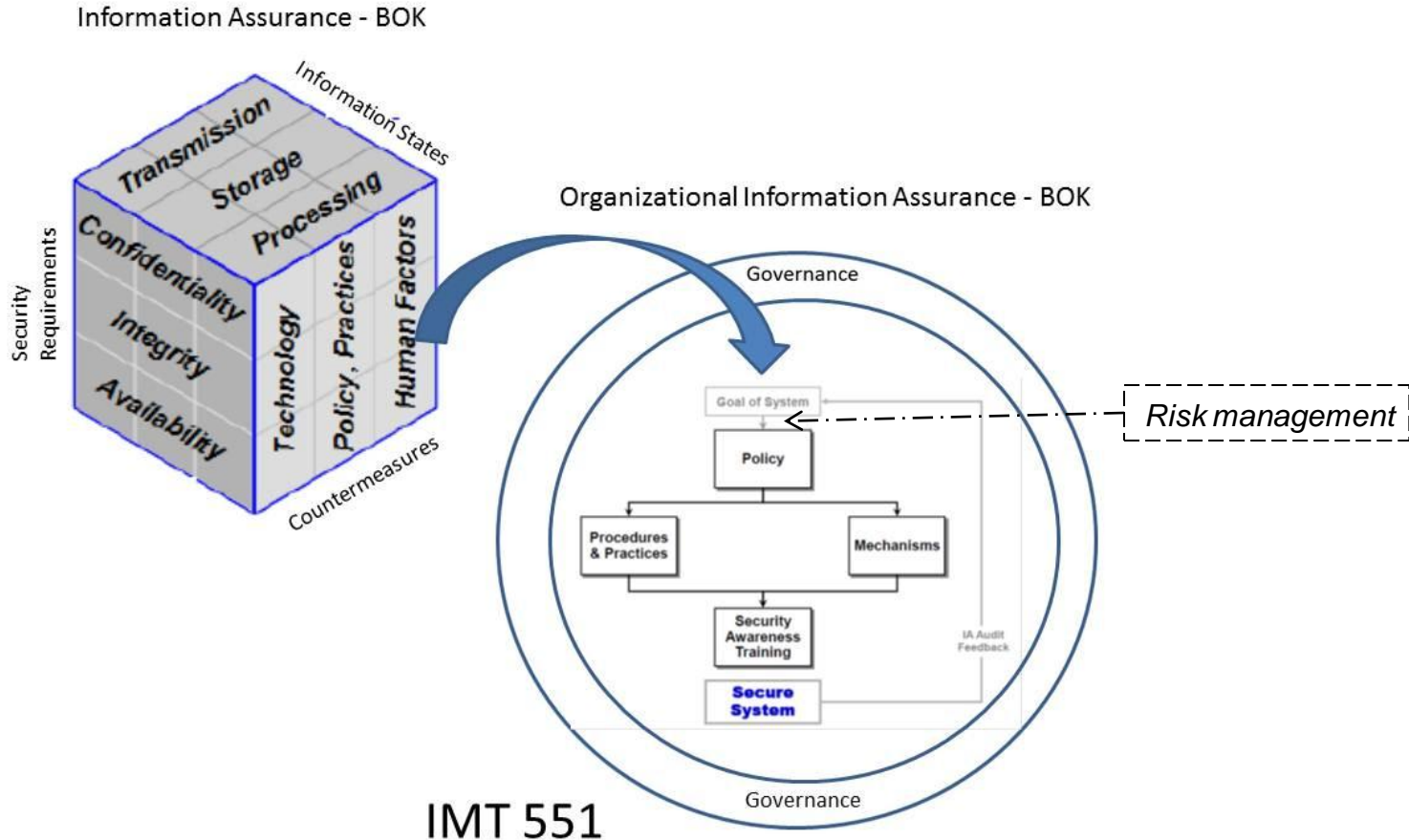
Multi-disciplinary, Cross campus

CIAC ACADEMIC OFFERINGS

Multi-Disciplinary Applied Approach to Information Assurance

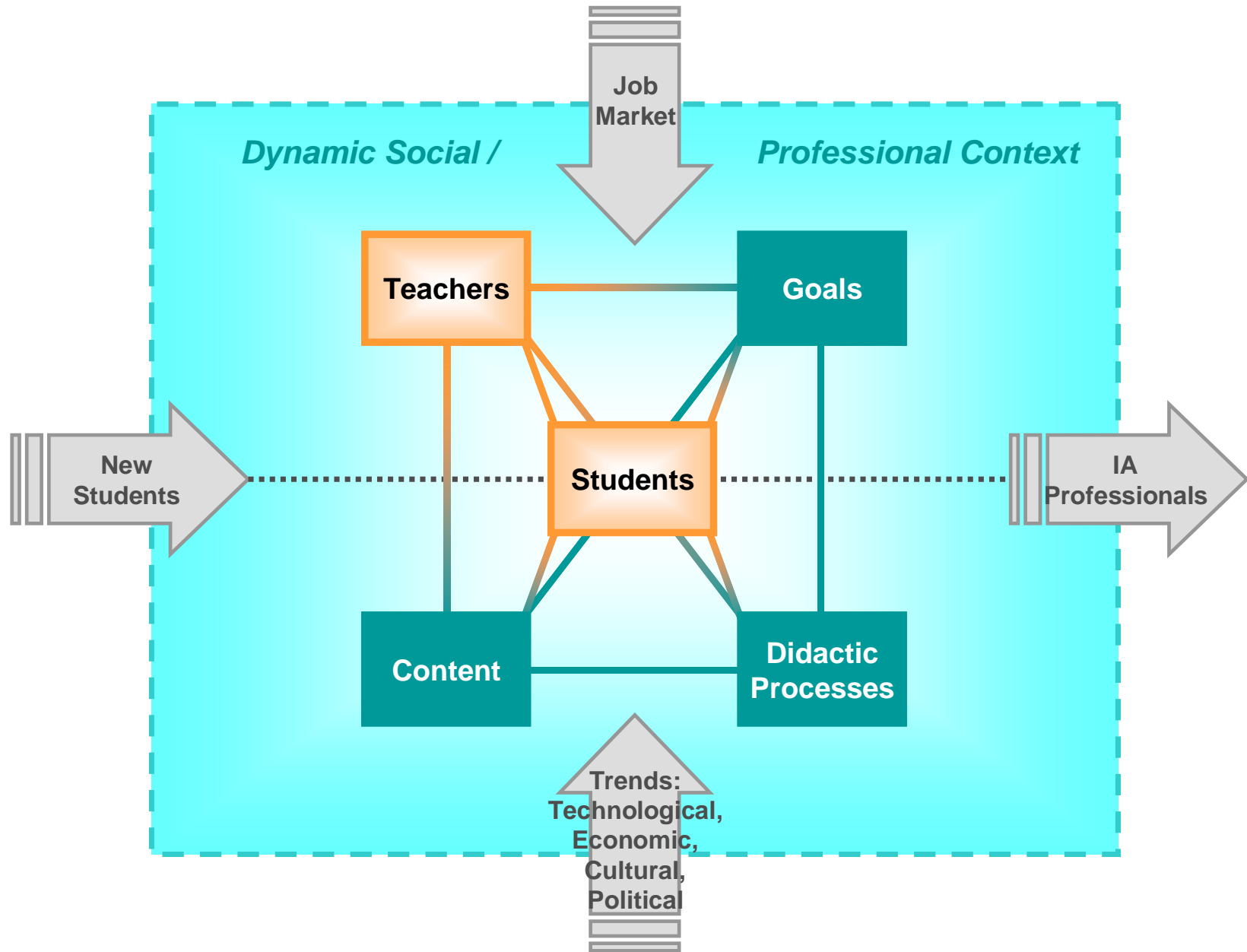


Content



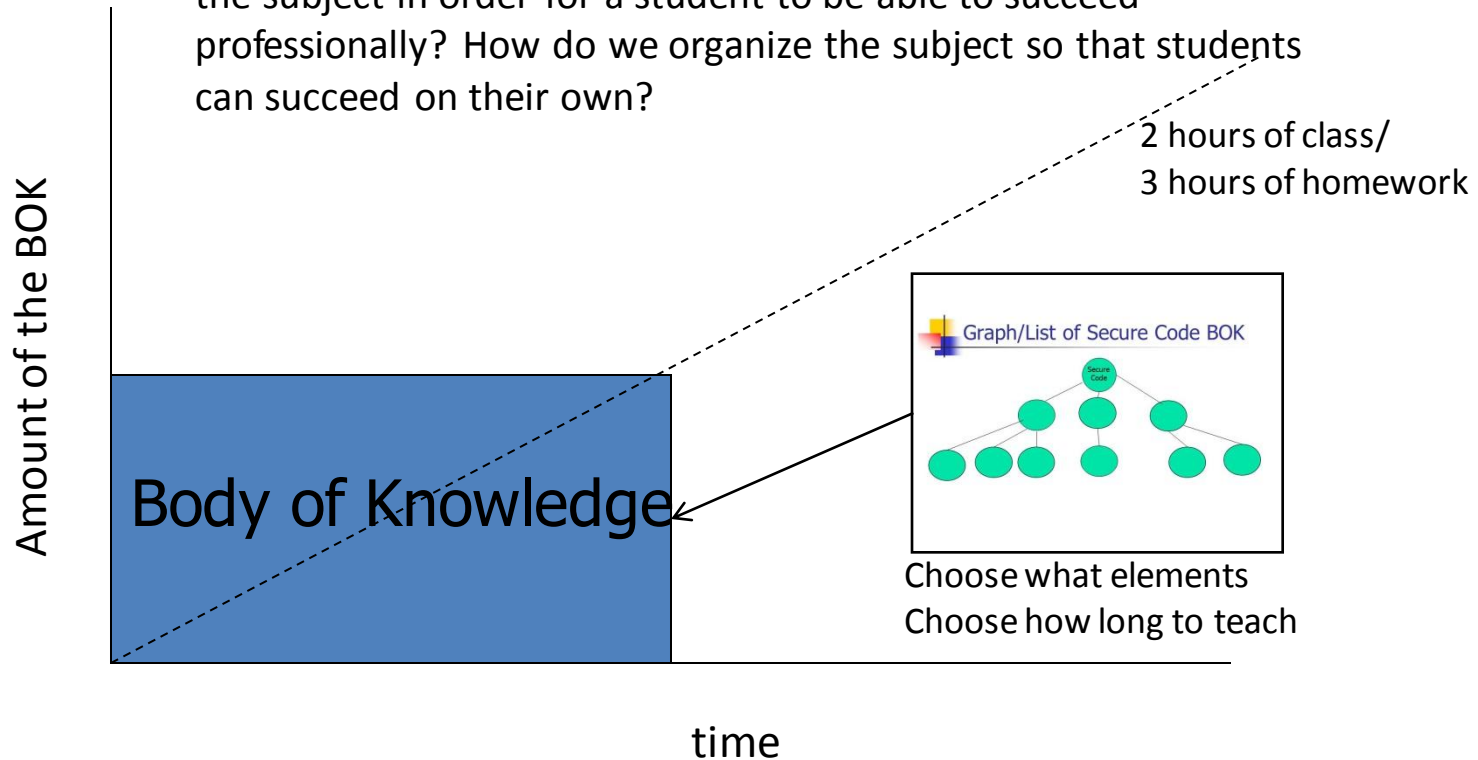
- No BOK for IA/IS
- CISO : ISRM as CEO : MBA
- Curriculum Framework

KBP Pedagogical Model for IA Curriculum Development



Task 4: Mini/Max Knowledge Model for Teaching a Subject

What minimal amount of knowledge should be taught about the subject in order for a student to be able to succeed professionally? How do we organize the subject so that students can succeed on their own?



Curriculum, Conferences & Workshops

- IA Certificate Programs (3 courses)
 - Information Systems Security (UWT, UW Seattle)
 - Information Security and Risk Management - (Cloud topics integrated)
 - Network Engineering
 - Digital Forensics (UWT, UW Seattle)
- IA Tracks/Electives
 - MSIM IA series and course modules
 - Informatics courses
 - MSCS – UWT courses (network and computer security, IA, secure coding)
 - MSCS – UWB courses (digital forensics, secure coding)
 - MIPM courses (IA, RM/Disaster Recovery)
 - PhD CS—IA course
- Unintended Consequences of Information Age Lecture Series (UWTV)
- UW Conferences and Workshops: CCSC, IRMSCI, ASTAR, NWSEC, NISTIR, Honeypots Wkshp
- Pacific Rim Collegiate Cyber Defense Competition

Well placed graduates

RESULTS

UW/IA Cohorts

Cohort	Academic Year	Certificate Students (female)	Matriculated Students (female)
I	2005	11	
II	2005-6	16 (5)	
III	2006-7	18	
IV	2007-9	19 (4)	16 (4)
V	2008-9	17 (5)	8 (3)
VI	2009-10	12 (4)	14 (4)
VII	2010-11	22* (5)	30* (8) (5 WNG)
VIII	2011-12	27 (5)	33 (12) (6 WNG)
		142 (19)	101 (31)

Sample success stories

- NCC Deputy Manager, National Communications System, Cybersecurity and Communications, US Department of Homeland Security— Mike Roskind
- CEO Honeynet Project – Christian Seifert
- Tech Dir NSA – Darren King
- CISO – Todd Plesco
- FSO BAH Seattle – Brian Haller
- Concise Consulting Founder and CEO— Aaron Weller
- BAH Senior Malware Consultant—Remy Baumgarten
- IA audit, system and risk analysts
- Research scientists

A Systematic Approach to
Information Systems Security Education

SYSTEMS ENGINEERING IN IA

Overview

Introduction

Comprehensive Model of Information Systems Security (McCumber Cube)

Asset Protection Model (APM)

Cognitive Complexity - Miller Index

Asset Cube

System – Systems Engineering Community

Target – Information Assurance Community

Threat – Justice, Legal and IC Communities

Information Systems Security Framework

System Framework

Target Framework

Threat Framework

Dynamic System Security Model

Preliminary Results from Team Use

Summary, Conclusions

Introduction

Purpose

- Establish an expanded conceptual model for asset protection

Constraints

- Human short-term reasoning capability
- Rate of technology and organizational change
- Involvement of multiple professional communities
- Expert knowledge differentiated from novice knowledge
- Lack of commonly accepted legal infrastructure

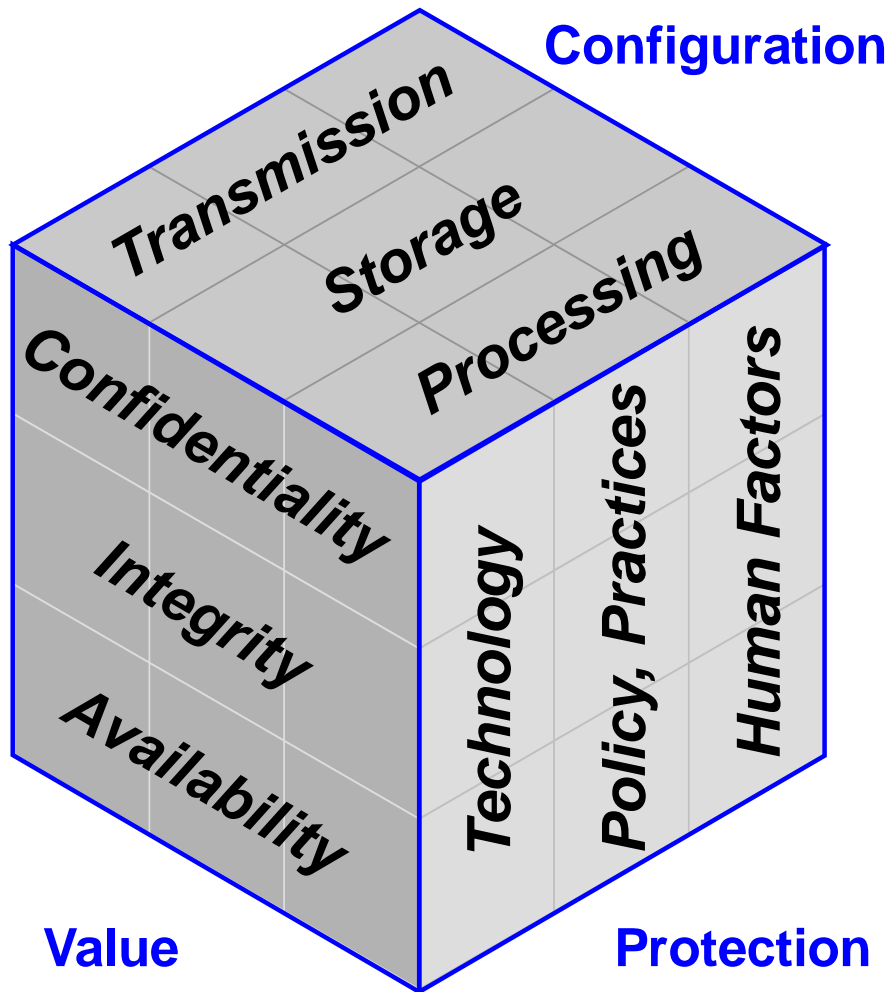
Proposed New Model

- Supports human reasoning capabilities
- Establishes recursively defined levels of abstraction
- Supports computer-enhanced reasoning at detailed level
- Implemented independent of organization and technology

Outcomes

- Conducted team test with CISO focus (one academic quarter)
- Strong positive feedback from team and instructor

McCumber Cube

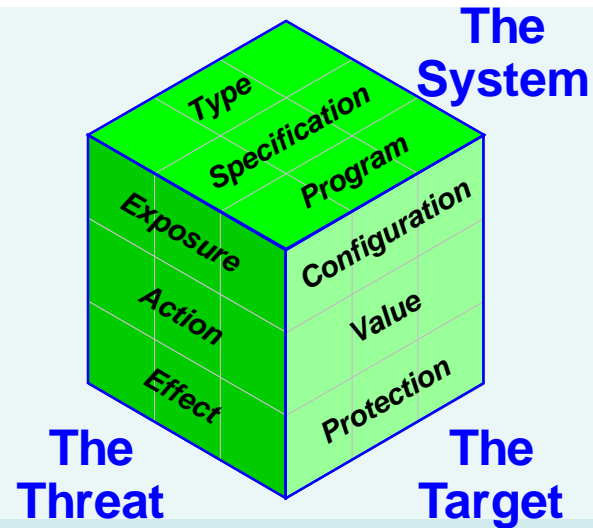


- Represents durable risk assessment model for information assurance (IA) community
- Configures to a 'matrix' of 9 elements
- Accommodates short-term human cognition capabilities
- Reflects structural design principles from systems science

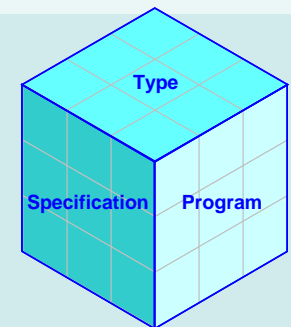
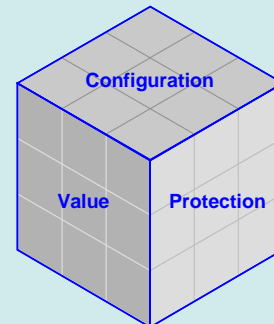
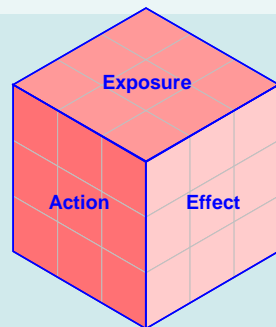
Asset Protection Model

Recursive design for adaptable computer support

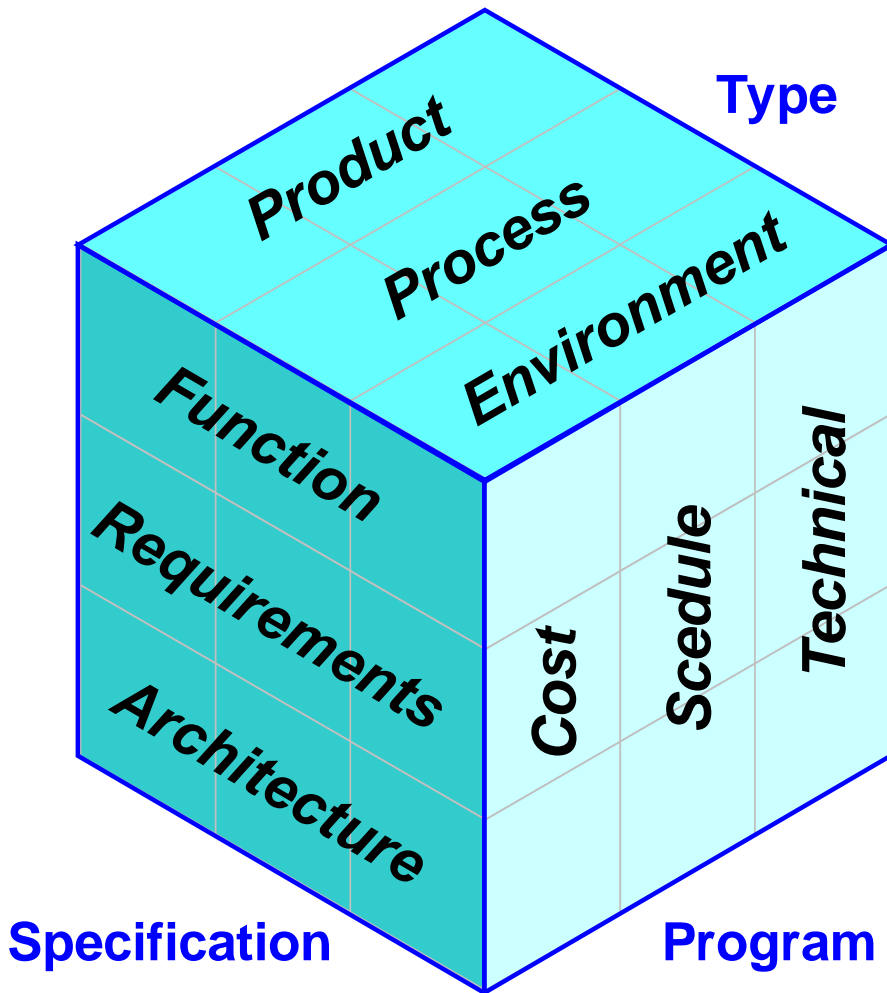
*Highest Level of
Abstraction – Level 1*



*Abstraction
Level 2*

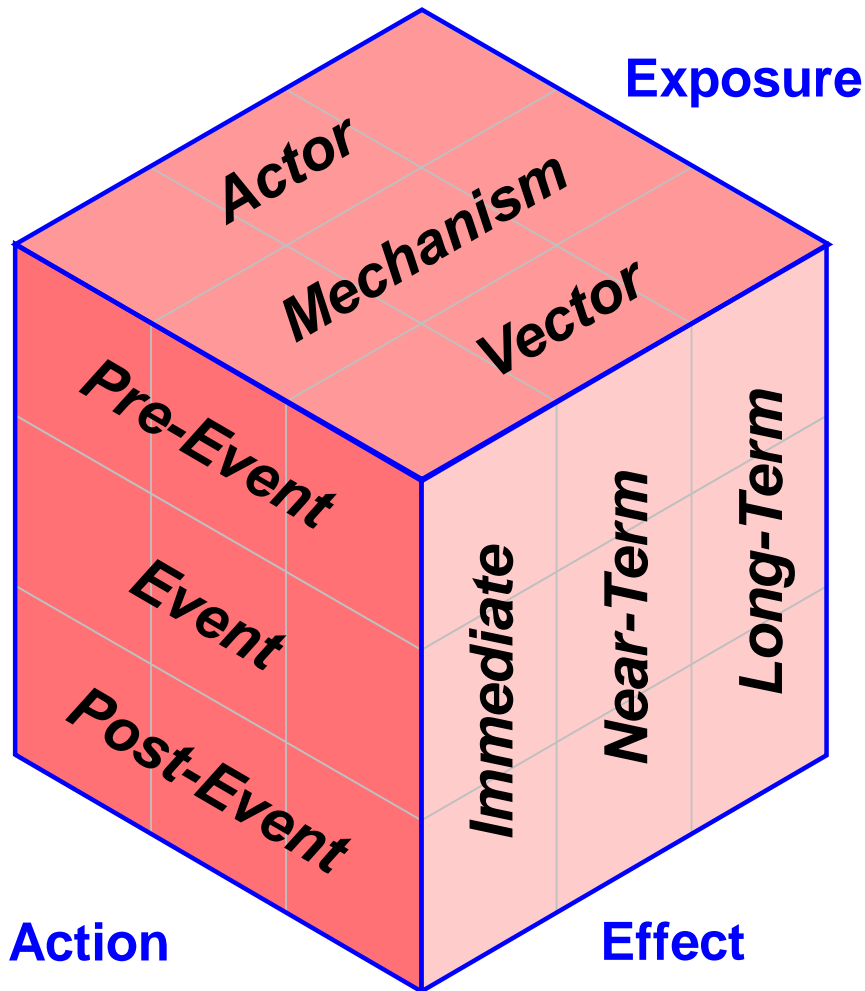


Asset Cube - System



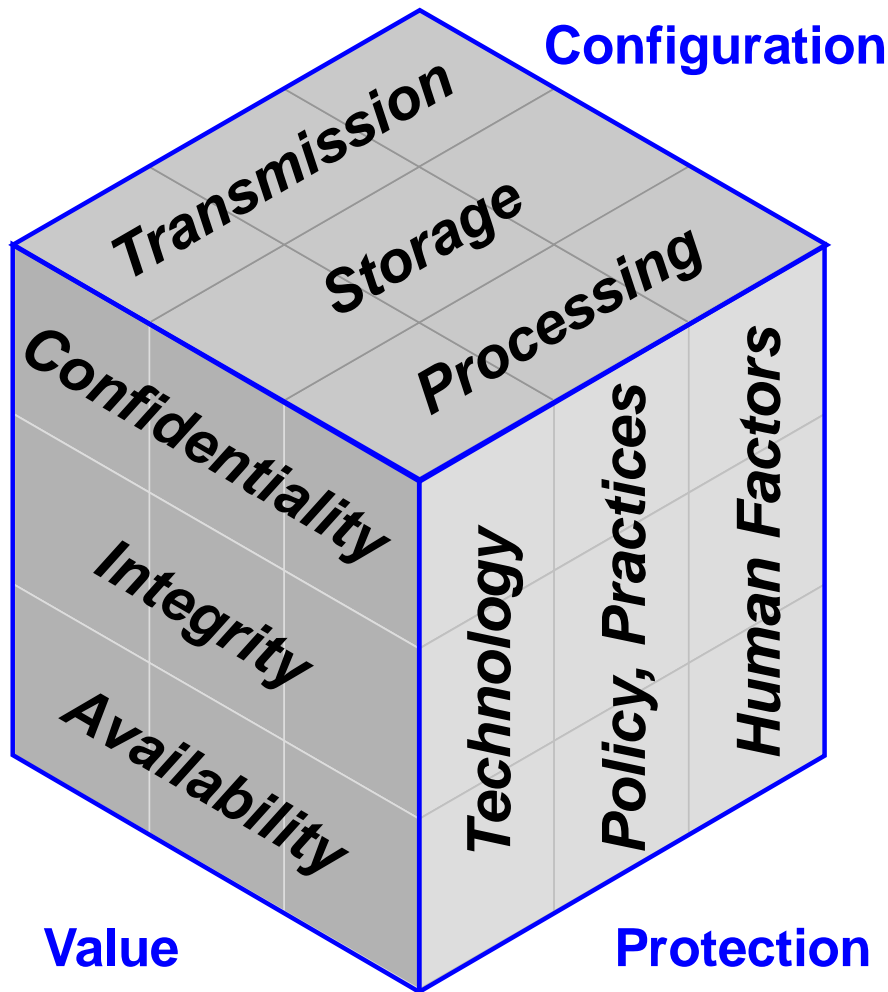
- Represents durable systems model for systems engineering (SE) community
- Configures to a 'matrix' of 9 elements
- Accommodates short-term human cognition capabilities
- Reflects structural design principles from systems science

Asset Cube - Threat



- Represents durable threat model for Justice, Legal, and IC communities
- Provides level of detail to support information classification
- Configures to a 'matrix' of 9 elements
- Accommodates short-term human cognition capabilities
- Reflects structural design principles from systems science

Asset Cube - Target



- Represents durable risk assessment model for information assurance (IA) community
- Configures to a 'matrix' of 9 elements
- Accommodates short-term human cognition capabilities
- Reflects structural design principles from systems science

APM Framework – ‘Sub-Cube’ Structure (1 of 3)

X Axis	Y Axis	Z Axis
System Type	Threat Exposure	Target Configuration
System Type	Threat Exposure	Target Value
System Type	Threat Exposure	Target Protection
System Type	Threat Action	Target Configuration
System Type	Threat Action	Target Value
System Type	Threat Action	Target Protection
System Type	Threat Effect	Target Configuration
System Type	Threat Effect	Target Value
System Type	Threat Effect	Target Protection

APM Framework – ‘Sub-Cube’ Structure (2 of 3)

X Axis	Y Axis	Z Axis
System Specification	Threat Exposure	Target Configuration
System Specification	Threat Exposure	Target Value
System Specification	Threat Exposure	Target Protection
System Specification	Threat Action	Target Configuration
System Specification	Threat Action	Target Value
System Specification	Threat Action	Target Protection
System Specification	Threat Effect	Target Configuration
System Specification	Threat Effect	Target Value
System Specification	Threat Effect	Target Protection

APM Framework – ‘Sub-Cube’ Structure (3 of 3)

X Axis	Y Axis	Z Axis
System Program	Threat Exposure	Target Configuration
System Program	Threat Exposure	Target Value
System Program	Threat Exposure	Target Protection
System Program	Threat Action	Target Configuration
System Program	Threat Action	Target Value
System Program	Threat Action	Target Protection
System Program	Threat Effect	Target Configuration
System Program	Threat Effect	Target Value
System Program	Threat Effect	Target Protection

APM Level 1 Interfaces

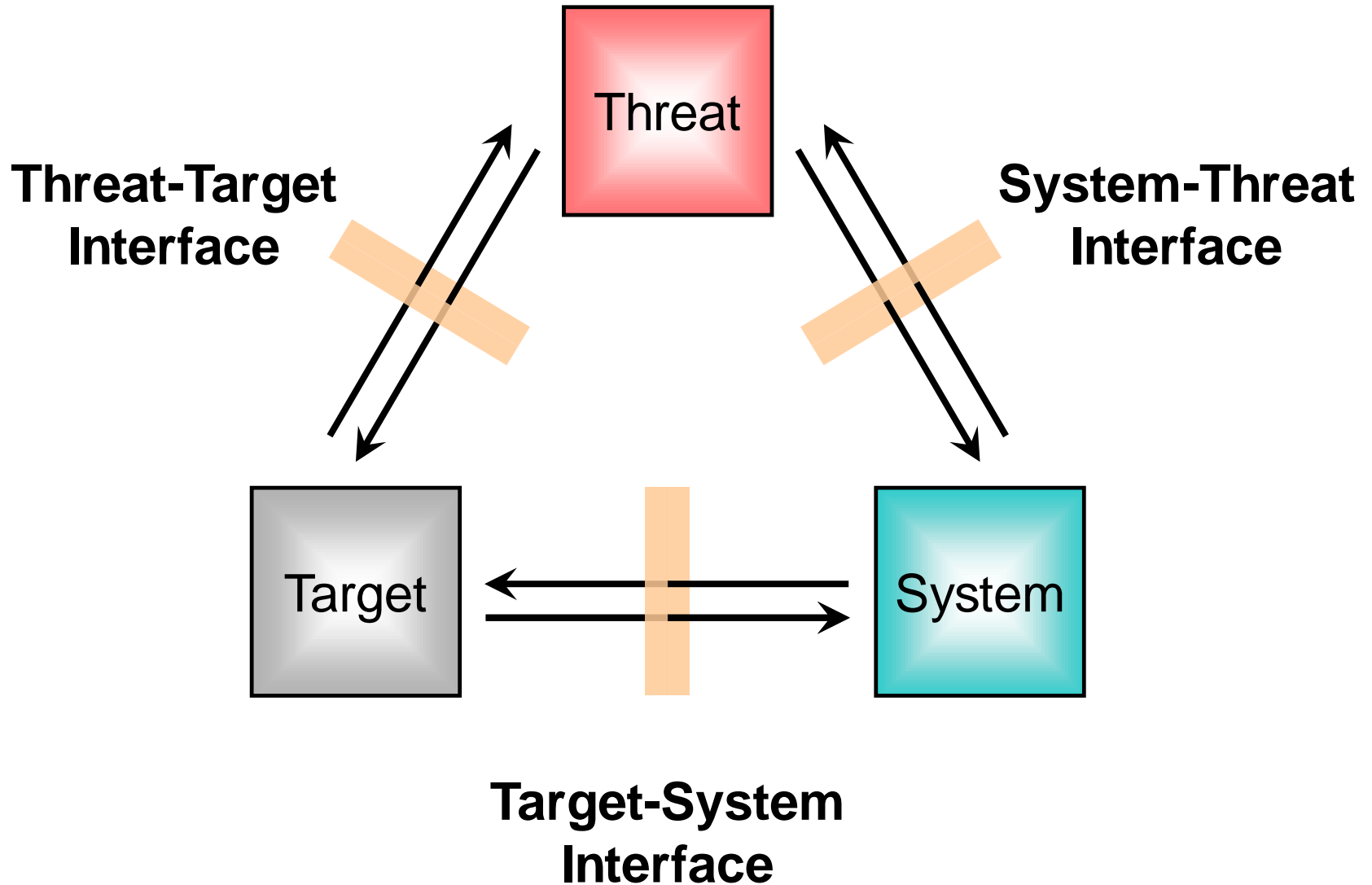
Interface Communications

- Well-defined interfaces with clear, structured patterns
- Experts can focus on their particular area of expertise
- Novices have a way of identifying where/why data contributes to their decision making

Level 1 Interfaces

- System – Threat Interface
- Threat – Target Interface
- Target – System Interface

APM Framework - Interfaces



APM Dynamic System Security Model

Existing Systems Dynamics Model

- Articulates the “arms race” between cyber attackers and cyber defenders
- Created using a high level of abstraction

State of System and Target Security

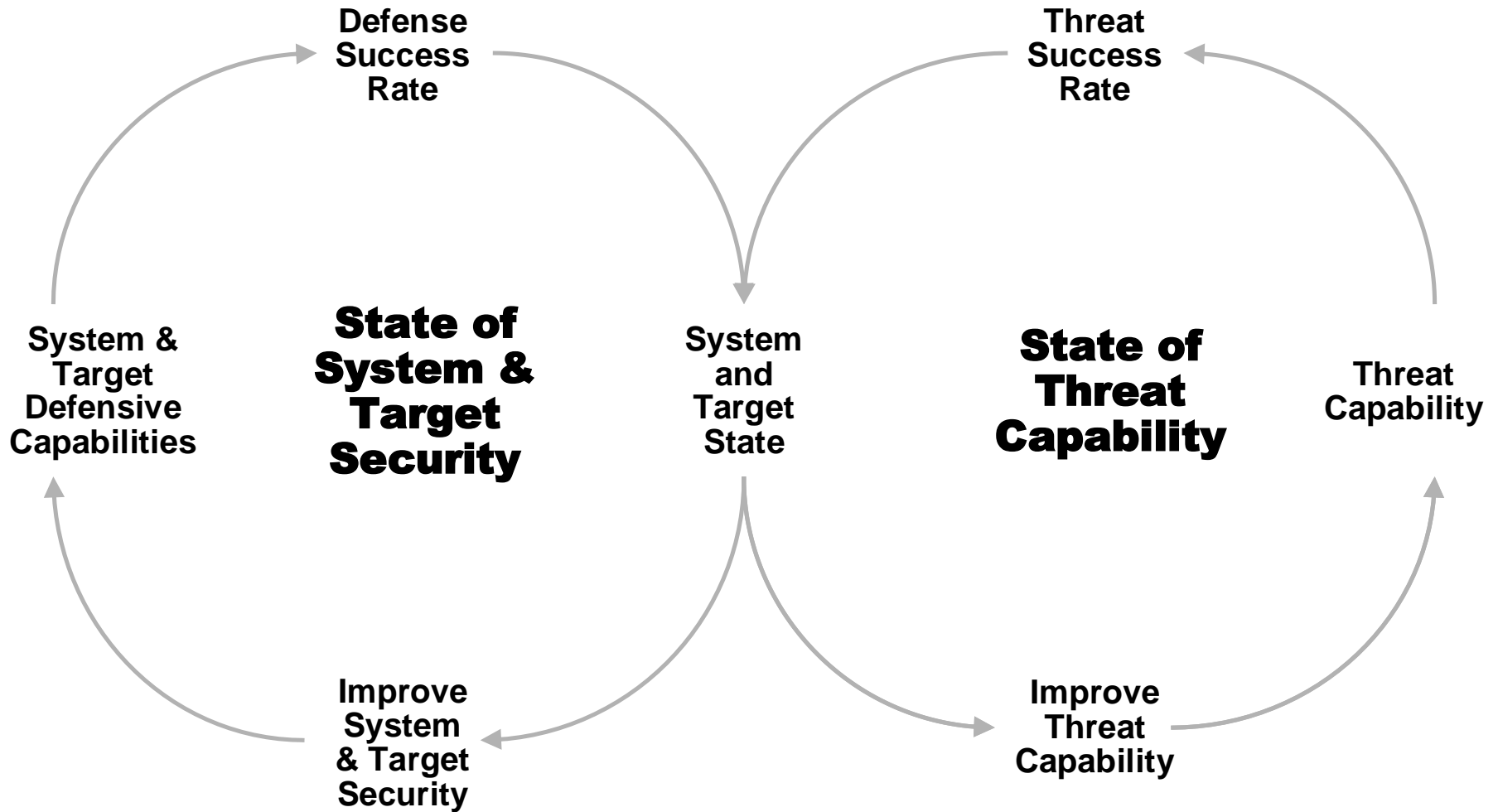
- System and Target Defensive Capabilities
- Defense Success Rate
- Improve System and Target Security
- System and Target State

State of Threat Capability

- Threat Capability
- Threat Success Rate
- Improve Threat Capability
- System and Target State

APM will provide the ability to build a more comprehensive dynamic systems security model

Dynamic System Security Model



Preliminary Results from Team Use (1 of 2)

Team objectives

- Understand the current state of cyber security incident reporting
- Determine the data quality associated with threat incident reporting
- Recommend methods for improved data quality collection

Asset Protection Model (APM) Application

- Used to organize a vast volume of existing data including:
 - Common Attack Pattern Enumeration and Classification (CAPEC)
 - Common Vulnerabilities and Exposures (CVE)
 - National Vulnerability Database (NVD)

APM Model Semantic Calibration

- Applied model to several standard non-cyber security threat instances
 - Bank robbery – threat actor, threat mechanism, threat vector
 - Car hijacking – threat actor, threat mechanism, threat vector
 - Terrorist attack – threat actor, threat mechanism, threat vector

Preliminary Results from Team Use (2 of 2)

Team APM Model Utilization

- Used to place incident data in context of cyber security
- Guided team judgments regarding applicability, quality of the data
- Supported analysis of information gaps and poor data quality

Team Results

- APM provided a structural context that could be analyzed by experts from a particular field
- Structure allowed communication of data between novice and experts
- APM viewed as effective
- APM provided structure needed to organize existing cyber security incident data
- Threat Cube concepts supported categorization, and definition of interrelationships between common threat types and attack patterns

Summary, Conclusions

The Asset Protection Model (APM)

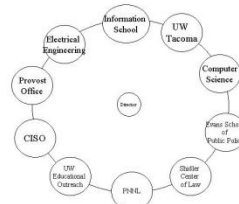
- Establishes modules that allow internal controls, with communication and interaction at the interfaces
- Supports recursive definition of levels of abstraction
- Provides a focal point for the key asset protection communities – the IA, Systems, and Justice/Legal/IC
- Establishes a common framework for tailoring curriculum based on changes in technology and the threat spectrum
- Supports dynamic analysis of specific types of cyber defense activities
- Supports both human short-term cognition, and computer-enhanced reasoning methods
- Is independent of specific organizations and technologies, and will remain stable for an extended period of time

**More Research Is Needed to Refine the APM
Concepts, and Its' Applications**

Multi-disciplinary, Cross campus, International

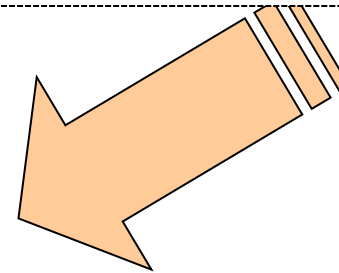
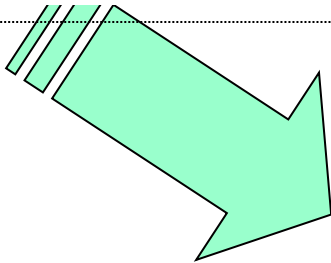
CIAC RESEARCH

CIAC Research Collaboration Conceptual Model



Schools/Depts.
Independent Research

External Partners



Governing Board

Exec Steering Committee

Research Dissemination

Rapid Research Response

Baseline Funding

Lecture series
IA Conference
Publications

Policy

Procedures

Technology

Ed/Awareness

Current Center Activities

Funded Projects

Next Generation Honeypots

Assessment of using virtualization for network instrumentation, incorporating deception into next generation honeypot design.

Secure Coding Project

Piloting secure coding curriculum into CS programs in Puget Sound, reaching over 1200 students. Once externally evaluated, modules will be disseminated inside and outside the region.

Veterans Transitioning Studies

Pilot project facilitating veteran transition from military to academic life—specifically IA studies.

IA Compliance Framework

A lack of regulatory controls in China has focused outsourcing on this growing challenge. An IA governance framework, adapted from industry, is proposed as a control to mitigate.

Cyber Competition (PRCCDC)

Regional Cloud virtual laboratory

White Papers

Enterprise Governance in the Cloud

--NISTIC

--NSF SaTC

-- Further development of UK Cloud toolkit

Cyber Warrior

Defining recruiting profiles, mentoring and mgmt. strategies for cyber defenders

Smart Grid

Various cybersecurity issues

Risk Management

Comparing IA risk management with approaches in other industries

Systems Engineering in IA

Developing implementation models for allocating systems engineering goals throughout an organization.

Virtual World Security

Defining and developing Virtual World security awareness training in 2nd Life

IPSEC Interoperability-Boeing

Reconciling IETF RFC's, implementing IPSEC procedures, recommending best practices

Transitioning America's Veterans to STEM Academic Programs



Case Studies

Explore challenges
Model success



Project Report

Establish pipeline
Build program foundation

APPROACH

Assistance and encouragement to transitioning veterans, members of the National Guard and reservists with entering into academic programs, particularly those in STEM fields of study.

Pilot Program



Math boot camps

Industrial Committee

Buddy System

Student Preparation and Mentorship

Plans for accommodation of students with disabilities

Collaborations and Partnerships

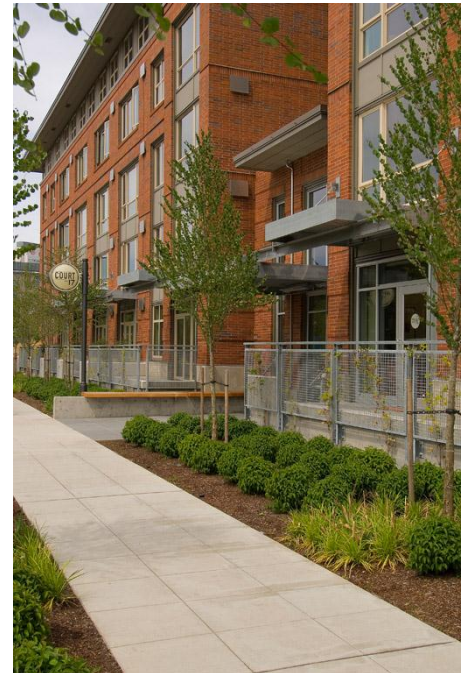
Honor House at UW Tacoma

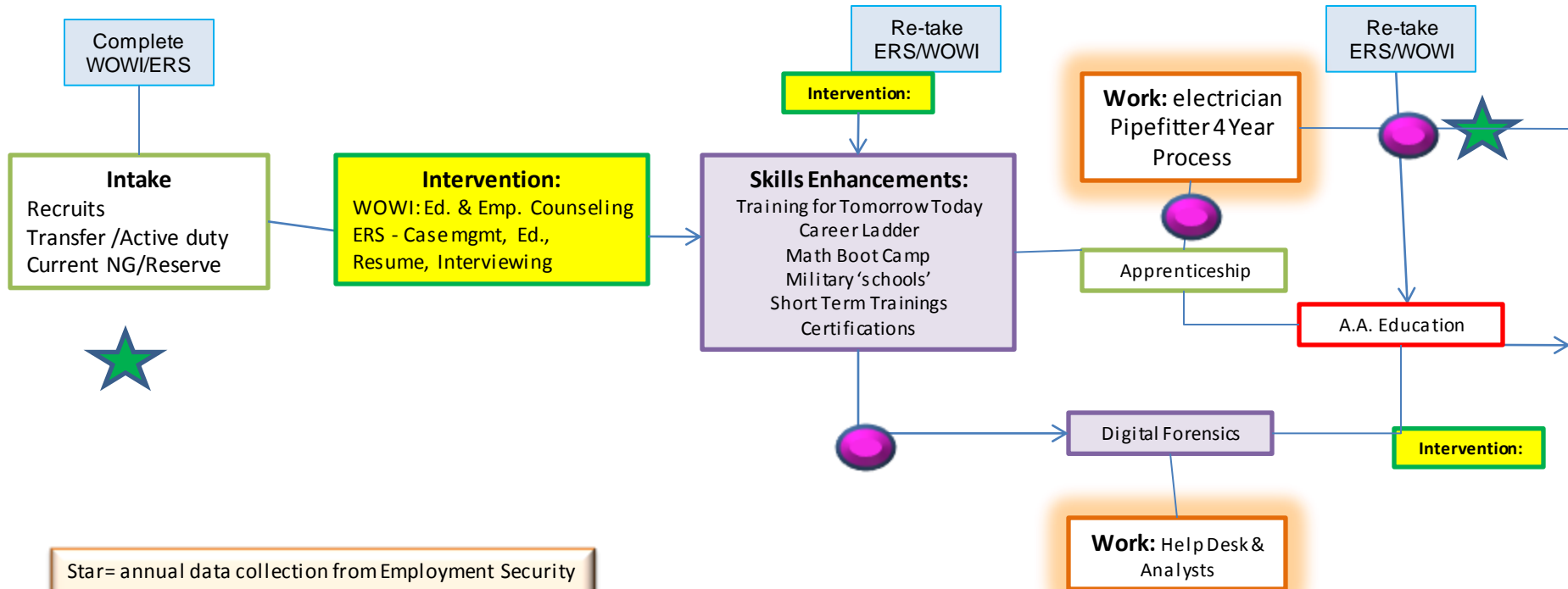
Court 17 as home to:

- Scholarship for Service: Expansion to the undergraduate programs
- Institute Resident Scholars: Industry-based competitive housing/tuition aid
- Pierce County Honours House for new veterans and their families

<http://court17apts.com/>

- Tri-Campus IA and Cyber Security Program
- National Security Systems (CNSS) Training Standards
- Post-docs thru Endowed Professorship in Information Systems and Security





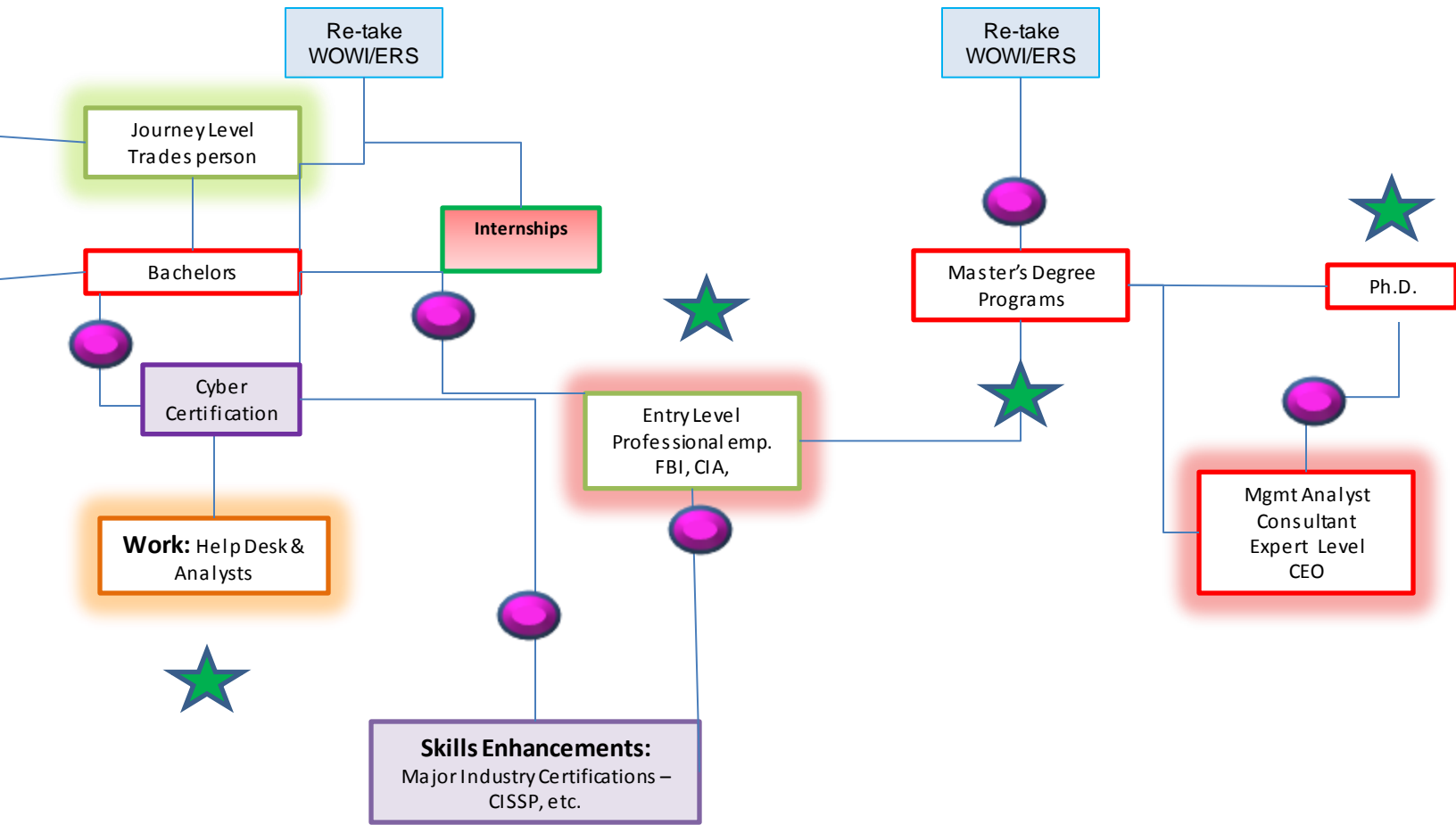
★ Star= annual data collection from Employment Security Dept. measuring income of all National Guard/Reserve members in WA. Flag SSN of NSF/STEM participants to measure impact of income/retention in NG.

ERS – given every six months for the first 3 years of program or after significant interventions or major deployments. Exact points to be determined.

WOWI – administered after significant educational and skills enhancements or after major deployments.

“Glow” Boxes indicate irrigation points ; individuals at this point may temporarily or permanently exit the pipeline.

● Circles: Indicate key stages for development and delivery of mentors for Veterans/NG passing through the system. Initially by industry people, eventually by Veterans for Veterans.



Branding activities

CIAC OUTREACH



ICIW 2012

22-23 March, Seattle, USA

Home >> ICIW >> ICIW 2012 >> ICIW 2012 home page

www ACI At a glance Calendar RSS Feed Contact us

- ICIW 2012 Home
- Call for Papers
- Submission Guide
- Abstract Submission
- Proof Reading
- Committee
- Abstracts Selected Programme
- Registration
- Practical Information
- Proceedings 2011
- ICIW Past & Future
- Seminars
- Advertisers
- Exhibitors
- Publishers
- Sponsors
- About ACI
- Academic Bookshop

- conferences
- publications
- e-journals
- seminars
- academic talk

7th International Conference on Information Warfare and Security ICIW-2012

Center for Information Assurance and Cybersecurity
 University of Washington, Seattle, USA
 22-23 March 2012

- Conference Chair:** **Dr. Barbara Endicott-Popovsky**, Center for Information Assurance and Cybersecurity, University of Washington, Seattle, USA
- Programme Chair:** **Dr. Volodymyr Lysenko**, Center for Information Assurance and Cybersecurity, University of Washington, Seattle, USA
- Keynote Speakers:** **Kirk Bailey**, CISO, University of Washington, Seattle, USA
Dr. Eneken Tikk-Ringas, University of Toronto, Munk School of International Affairs, Toronto, Canada

The conference will address elements of both theory and practice of all aspects of Information Warfare and Security, and offers an opportunity for academics, practitioners and consultants involved in the domain to come together and exchange ideas. The programme for the event will include an extensive range of peer-reviewed papers, including presentations from leaders in the field.

The ICIW has consistently managed to bring together a variety of people from different countries, backgrounds and experiences.

We hope that you will be able to be part of ICIW 2012 and we look forward to welcoming you to Seattle.

Barbara Endicott-Popovsky
 Conference Chair



follow us on
twitter
 Tag: #ICIW

Your contacts for this conference are:

- Programme Director: [Leigh Armistead](#)
- Academic enquiries: [Professor Dan Remenyi](#)
- Submission enquiries: [Charlotte Hall](#)
- Registration enquiries: [Charl Walters](#)
- Join the mailing list: [Mandy Butler](#)
- Other enquiries: [Mandy Butler](#)



Important Dates

- Abstract submission deadline: ~~12 September 2011~~ **Extended until 26 September 2011**
- Notification of abstract acceptance: ~~16 September 2011~~ **Completed**
- Full paper due for review: ~~20 October 2011~~ **Completed**



University Quad



Barbara Endicott-Popovsky



Volodymyr Lysenko



Kirk Bailey

Pacific Rim Collegiate Cyber Defense Contest (PRCCDC)

<http://www.uwtv.org/video/player.aspx?dwrid=27982>



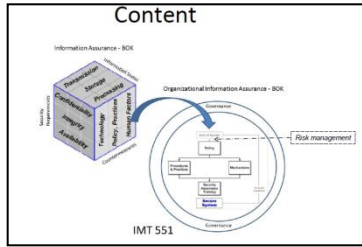
NOTE: UHM won Virtual Regional 2010; placed 2nd 2011
UW won Nationals in 2011

Welcome to Cybersecurity Island

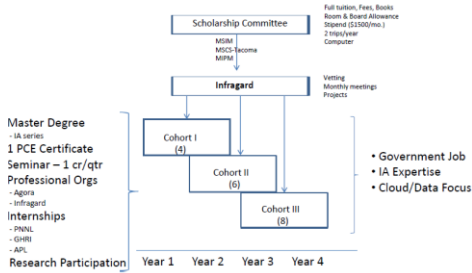
<http://www.youtube.com/watch?v=fvYOaf-9n-o>



INPUT

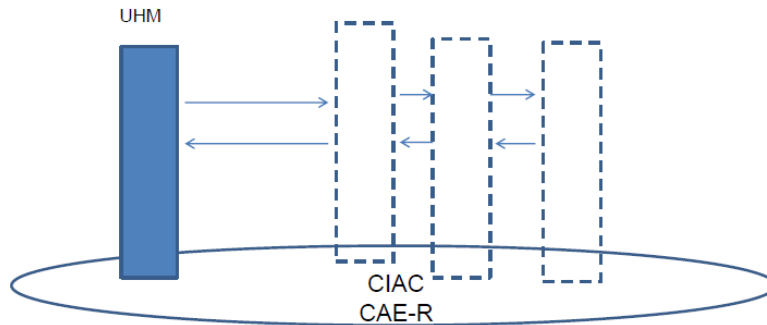
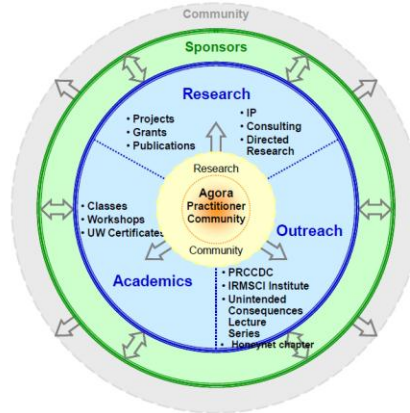


Managing Security in the Cloud:
Innovative Scholarship for Service Program



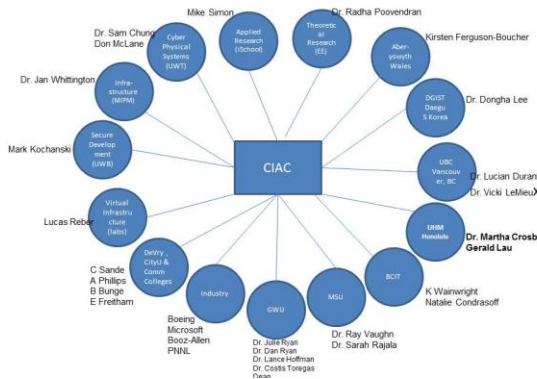
- Pentagon
- STEM-MSU
- Vets Engr
- Canada-BCIT
- UWT
 - Honour House
 - Degree
- Camp Murray: Morgan

CIAC



Symposia, Conferences, UW-TV Lecture Series, PRCCDC

CIAC Network of Collaborators



OUTPUT

Research

- Cloud
 - NISTIC
 - NFS/SaTC
- Smart Grid
- Health Sector
- Economics
- Secure Code
 - ACM 2013
- Law School Initiative
- Educational Initiatives
 - IA undergrad
 - UWT and UWB Masters
- CIAC NSA redesignation

System Engineering Possibilities

- Research—Sys Eng as the integrating discipline
 - Cloud
 - Smart Grid
- Education
 - Tool for our SFS students
 - PNNL requirements
- Outreach
 - Televised lecture
 - Honeynet Project

Challenges

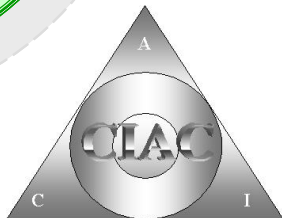
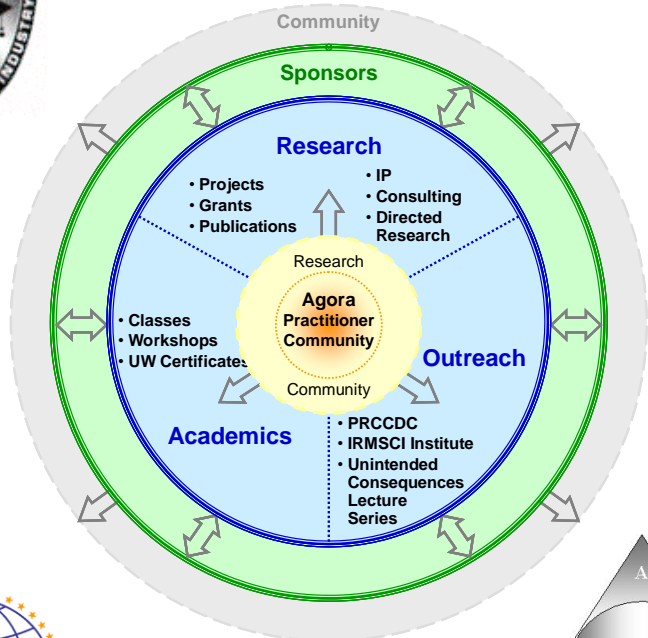
- Misperception of systems engineering
- Administrative resistance

Near Term Tasks

- Completion of this initiative
- Incorporation of system engineering into CIAC
 - Overview course required for all SFS students
- Grant funding

Leaders in IA: Securing the Future

Innovative Integration



- ✓ Key Collaborations
 - ✓ National Lab
 - ✓ Cross Domain
 - ✓ Cross University
 - ✓ Diverse Disciplines
- ✓ Emerging Technologies
 - ✓ Cloud, Smart Grid
 - ✓ Social Media
- ✓ Organizational & Technical Management
- ✓ Information Assurance Processes Toolkit

Math Bootcamp Approach

- Curriculum designed specifically for veterans
 - Multi-level format
 - Work at your own pace
 - Worked independently or in groups
 - Self-determined placement
 - Assisted by series of questions
 - Students allowed to adjust
 - Accommodated the injured
 - Online component to allow those injured to keep up
 - Attendance not required
 - Progress monitored
 - Daily check-ins
 - Group instruction on concepts 1-2 times per week

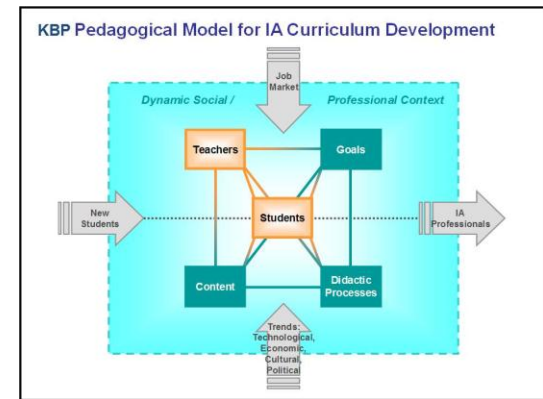


Figure 1. Participants are racially diverse

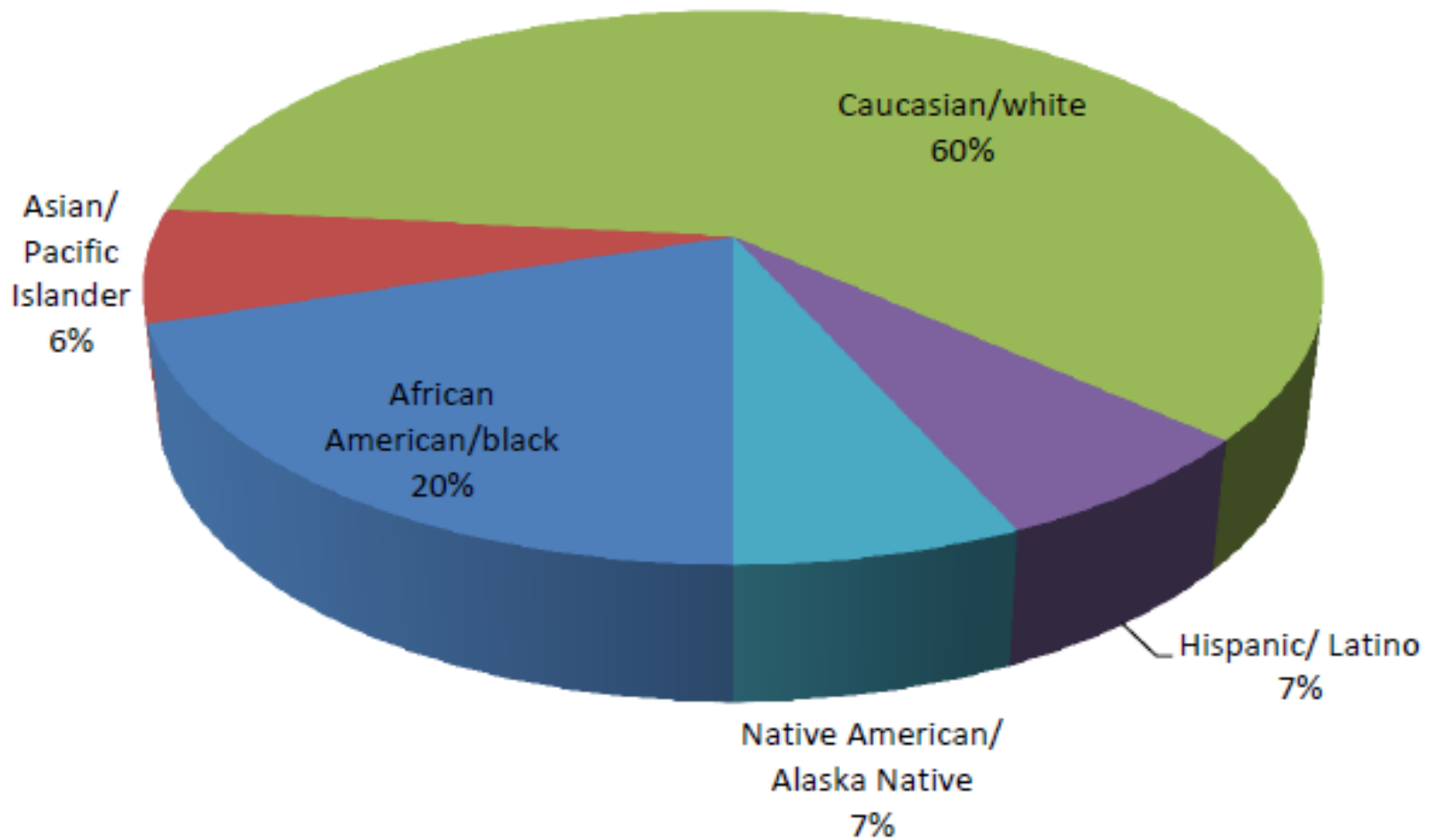
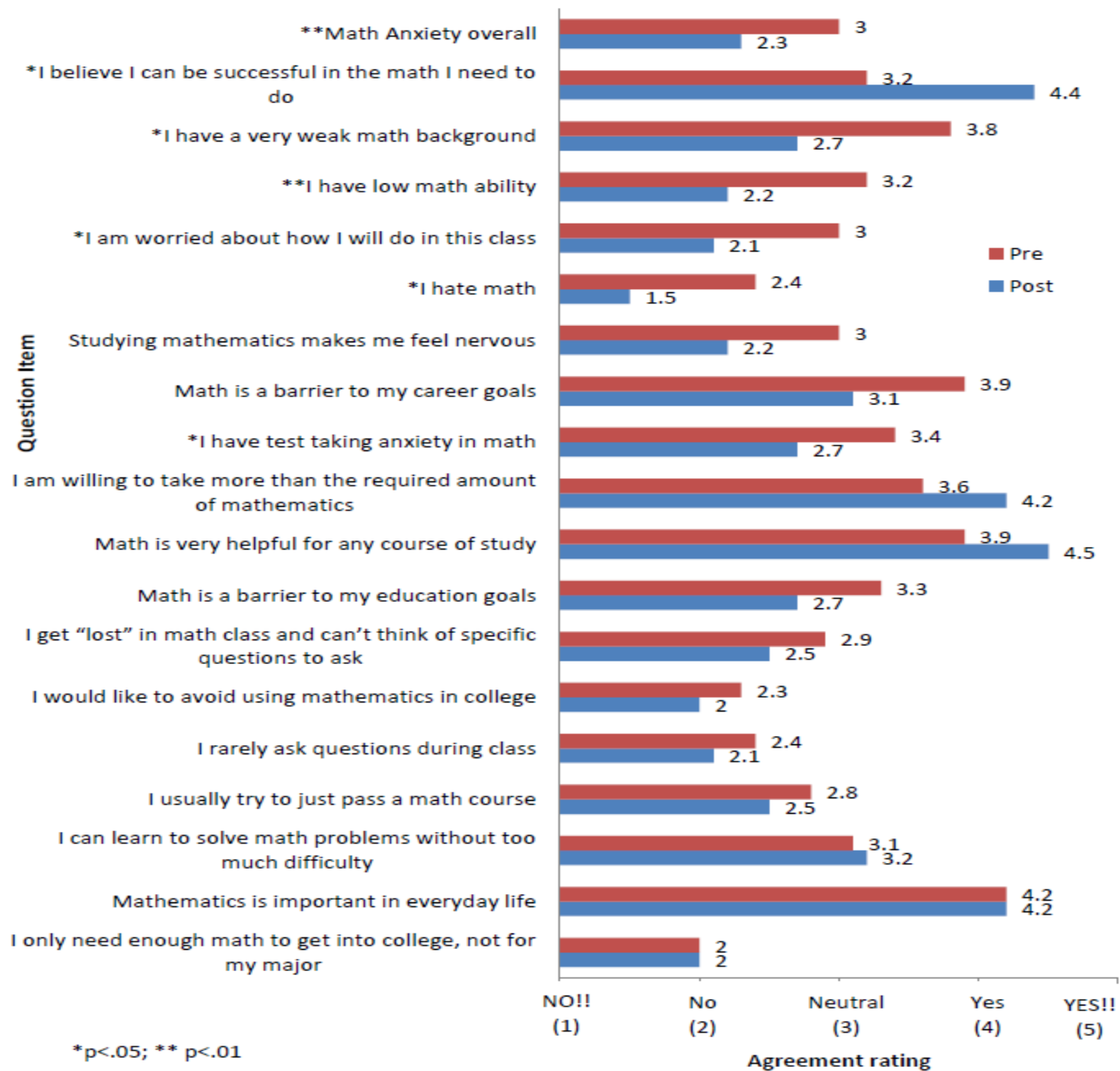


Figure 2. Change in math attitude



Verbatim Comments

- This class is giving the opportunity to excel faster in math to get to the college level calculus
- Gives me the confidence to tackle problems and knowledge to resolve them!
- I feel more confident
- Allowed me to feel I can succeed in math
- I have learned that it may not be as difficult as it may seem
- Knowing that teachers want to help is a great feeling
- This class has significantly boosted my confidence and ability to succeed in the accomplishment of this goal
- Math seems like less of an obstacle
- This class has helped me work through "shut down point" when I think I can't do it

Case Studies in IA Education

- Followed 5 National Guard thru IA education
 - Year long UW/CIAC/CNSS certification
 - Buddied up as a sub-cohort
 - Reinforced each other's experiences
 - Matched their background and interests
 - Natural extension of their WNG duties
 - Similarity in mission
 - Many civilian jobs available
 - Accumulated college credits
- Results
 - 2 of 5 transferred credits into MIPM degree program (brought 3 additional WNG into MIPM program)
 - 1 has taken a position full time in IA within the Guard
 - 1 completed his bachelors and this credential
 - 1 contemplating education options
- Recruited 7 for this year's IA program