



THE
GRADUATE
SCHOOL

Conflict Changing Curriculum

Dr. Loyce Pailen, CISSP

FISSEA Conference
March 15, 2015

Program Focus: New techniques for developing and
conducting effective, meaningful training and
education

Cybersecurity Management and Policy

President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation!

Whitehouse.gov



Cybersecurity Management and Policy Program

Introduction to Cybersecurity

Cybersecurity Management and Governance

Cybersecurity Risk Management and Compliance

Cybersecurity Program Development

Cybersecurity Capstone Simulation

The Curriculum Development Process: An Enhanced learning Model (ELM)

Begin with the
END:
Competencies



What students
must know and be
able to do

Craft: Learning
Demonstrations



Career/Field
relevant contexts
in which students
both learn and
demonstrate
their learning

Construct: The
Program



A mapping: if the
student has
successfully
completed all
learning
demonstrations,
they have also
mastered all
program
competencies and
are ready to
graduate

Highly-Aligned Programs for the Federal Workforce

Human Resource Management	Healthcare	Information Technology
Business and Management	Public Safety Administration	Cybersecurity
Acquisition and Supply Chain Management	Homeland Security	Project Management

“Competency-Based” Mastery of Skills versus Time in Class

Traditional Approach	Competency-Based Approach
Fixed Time	Variable time
Variable Learning	Fixed Learning (mastery)
Generalized Content	Personalized Content
Fixed Pace	Variable Pace
Varying student success	More student success

Who is This Program For?

Student(s)

Non-traditional

- Working adults

Military

- Active duty
- Veterans

Professionals

- Cybersecurity
- Information Technology
- Related fields

Career Changers

- Any field

Organization(s)

Military

- All services

Private Industry

- Small businesses
- Medium businesses
- Large businesses

Government

- Local
- State
- Federal

Non-profit

- All categories

What the Student in this Program will be able to do...

What we call “competencies”

- ▶ Know terms and technologies in order to assess cyber management and policy needs.
 -
- ▶ Design cybersecurity strategies that outline the vision, mission and goals aligning with the organization’s operational and strategic plans.
- ▶ Ensure the existence and understanding of a cybersecurity governance framework which includes the appropriate regulatory and compliance aspects.
- ▶ Address cyber attacks at the enterprise, national and international levels to correctly describe and discuss the cybersecurity technologies and policies that can effectively counter cyber attacks.
- ▶ Minimize risks to an organization’s cyberspace and prevent and/ or respond to a cybersecurity incident.

How We Validated the Program

Subject Matter Experts

- Working in the field
- Experience in industry
- Experience in government
- Experience in the military

Industry & Government Models

- Cybersecurity Industry Model – DoL
- National Initiative on Cyber Education – NIST
- National Initiative for Cybersecurity Careers & Studies – DHS
- DoD 8570 – DoD

Advisory Board

- Cybersecurity Advisory Board
- Cyber Curriculum Advisory Council
- Validators
- Focus Groups

Academia and Certifications

- University Sources
 - Program Chairs
 - Collegiate Professors
 - Adjunct Professors
 - Vice Deans
- CISSP
- CISM

Challenges

- ▶ Commitment from the Institution
 - Substantial Investment
 - Change in Philosophy
 - Different Business Model
- ▶ Use of Technology
 - Online environment and delivery
 - Scaling Tools
 - Analytics
 - Student Progress
 - Remediation
 - Threshold assessment


Challenges, cont'd.

- ▶ Shift for students
 - Independence
 - Research
 - Self-pacing
- ▶ Different way of teaching
 - Coaching and Mentoring
 - Subject-Matter Expert
 - Assessor
 - Persistence
- ▶ Resistance to change
 - Less traditional path to a college degree

Bottom Line

“Students are more marketable as mastered competencies are highly relevant to employers, and directly transferable to the workplace.”

Is this the right
direction for academia
to take?



How this Program is Better than Its Competitors

- ▶ Creates context through scenarios and real world applications – state-of-the-art tools
 - Enable students to attain mastery
 - Translate skills from classroom to work place
 - Competitors: No emphasis on tools of the trade
- ▶ Uses a multidisciplinary approach to provide both breadth and depth
 - Incorporates critical infrastructures and industry-specific focus
 - Competitors: depth or breadth
 - Competitors: management only
- ▶ Designed specifically to meet the needs of industry & government
 - Continuous evolution
 - Competitors: litany of courses from other programs

The “Program Elevator Pitch”

- ▶ Providing a state-of-the-art curriculum that is based on real world scenarios & techniques, and hands-on tools, used in today’s organizations
- ▶ Preparing students with cybersecurity knowledge and skills that are immediately applicable to the work environment
- ▶ Scholar-Practitioners working in the cyber field
 - CIOs, CISOs, CTOs, Executives, Managers, Engineers, Computer Scientists, Cyber Analysts, etc. - real world perspectives
- ▶ Multidisciplinary Approach to learning and mastery – Enhancing Learning Model
- ▶ Designated as a National Center of Academic Excellence in Cybersecurity and Information Assurance by the National Security Agency & Department of Homeland Security