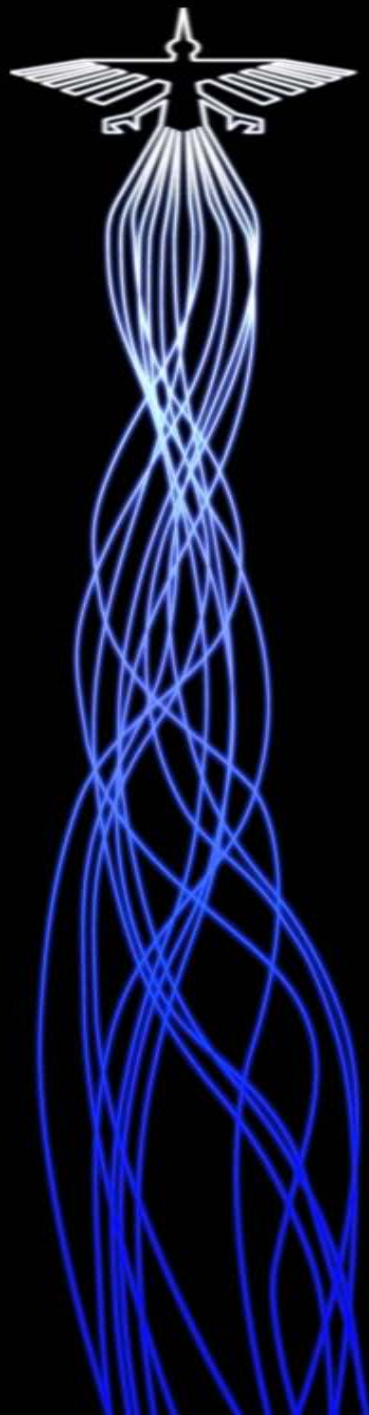
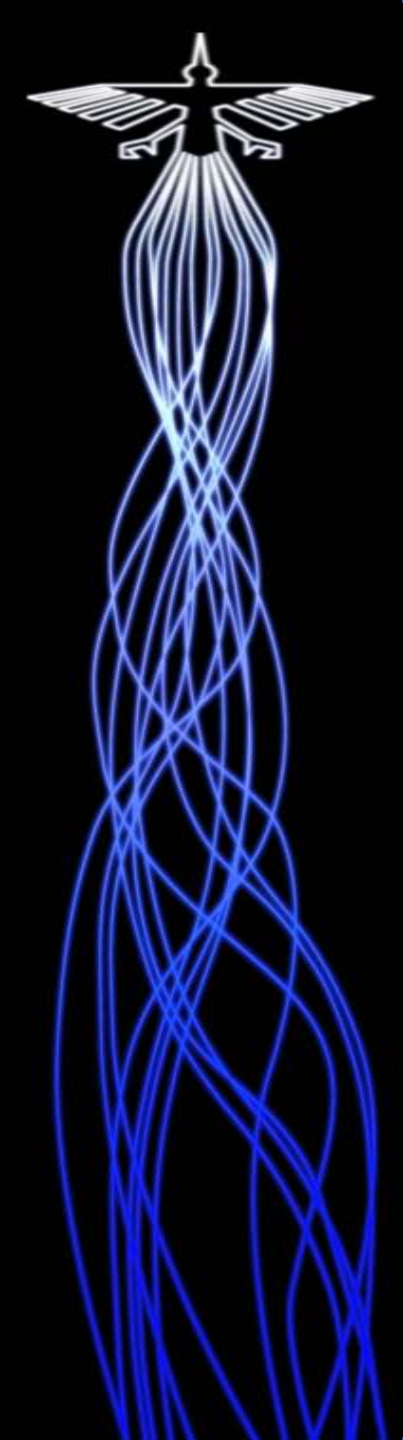


Moving Secure Software Assurance into Higher Education:

A Roadmap for Change

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



The Issue

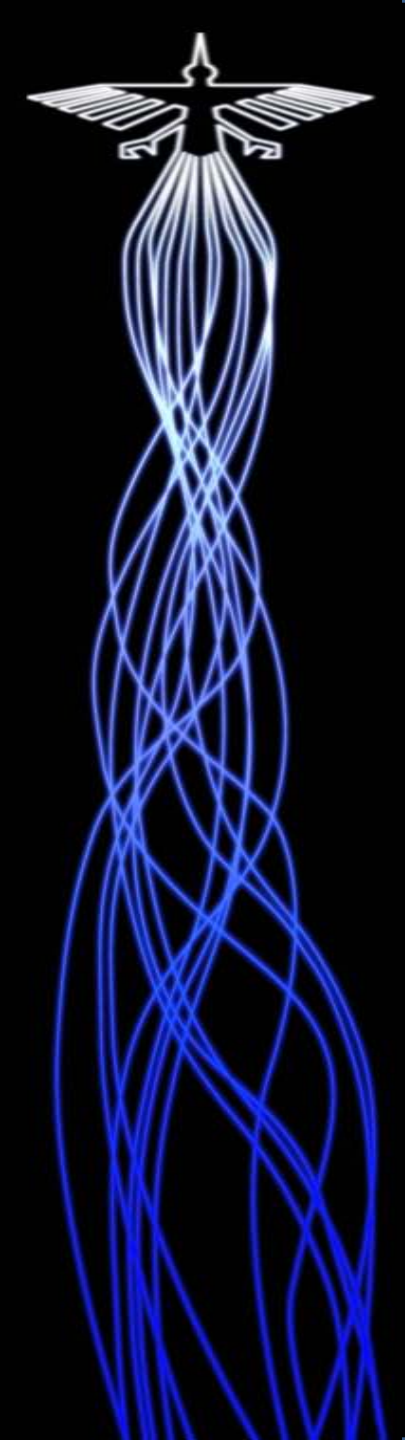
Software defects are avenues of attack that criminals, terrorists, or hostile Nations can exploit.

Since software defects are a historical given the entire industry will have to alter its behavior in order to have effective change

The only way to get leverage for such massive social change is through formal education programs

These might start as low as middle school and articulate upward all the way to advanced graduate study

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



The Current Problem in Education

Up to this point we have fully understood the shape of the field

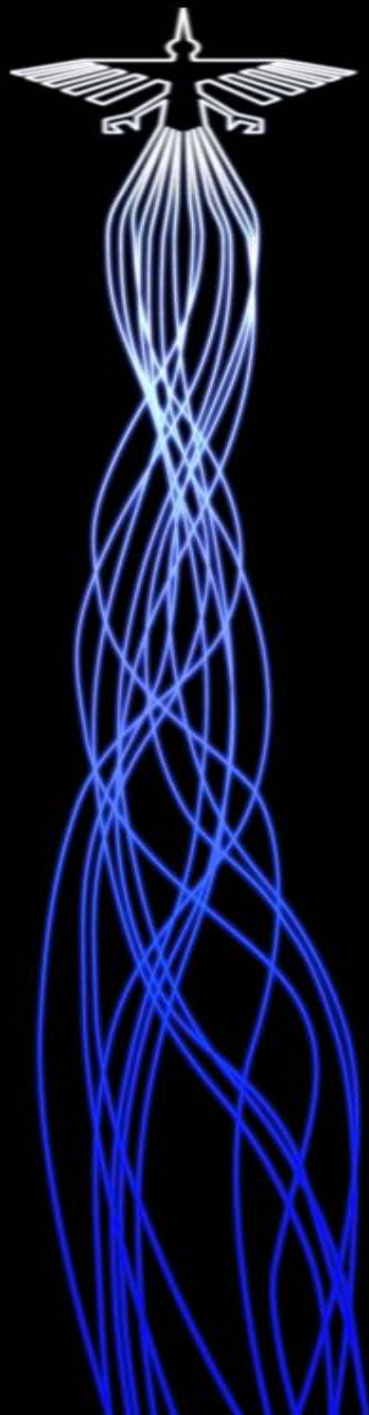
That is, there was no common agreement about the activities that might legitimately comprise a SwA curriculum

-Most SwA knowledge used to be called SQA – what's the difference?

-There are at least five different disciplines involved,

- Computer Science
- Software Engineering
- Information Systems
- Information Technology
- Information Assurance

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



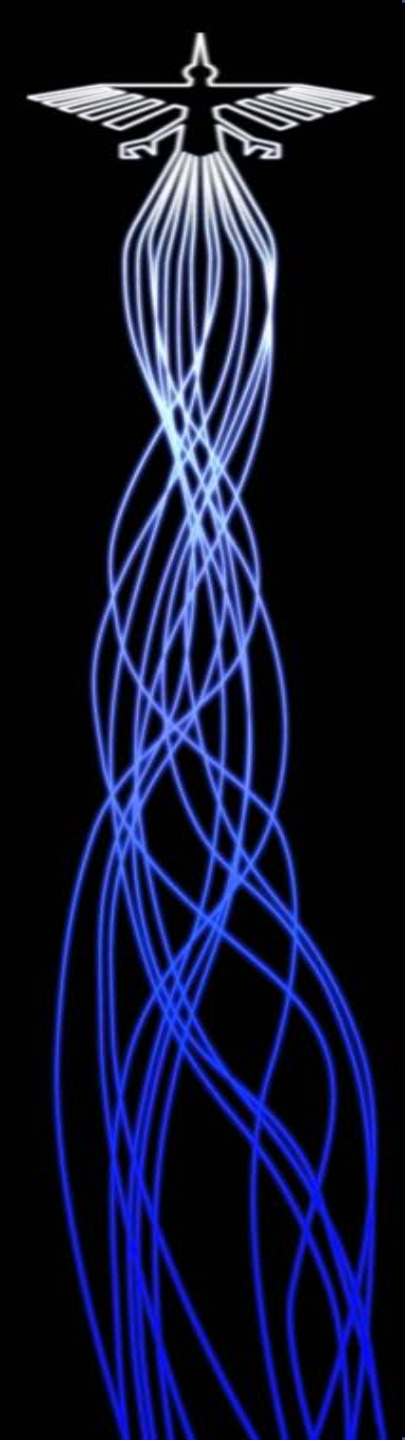
Some More Problems with Education

Essential SwA knowledge is cross cutting

It is generally agreed that some requisite SwA knowledge might be found in at least:

1. software engineering
2. systems engineering
3. information systems security engineering
4. safety and security
5. testing
6. information assurance
7. law
8. project management.

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



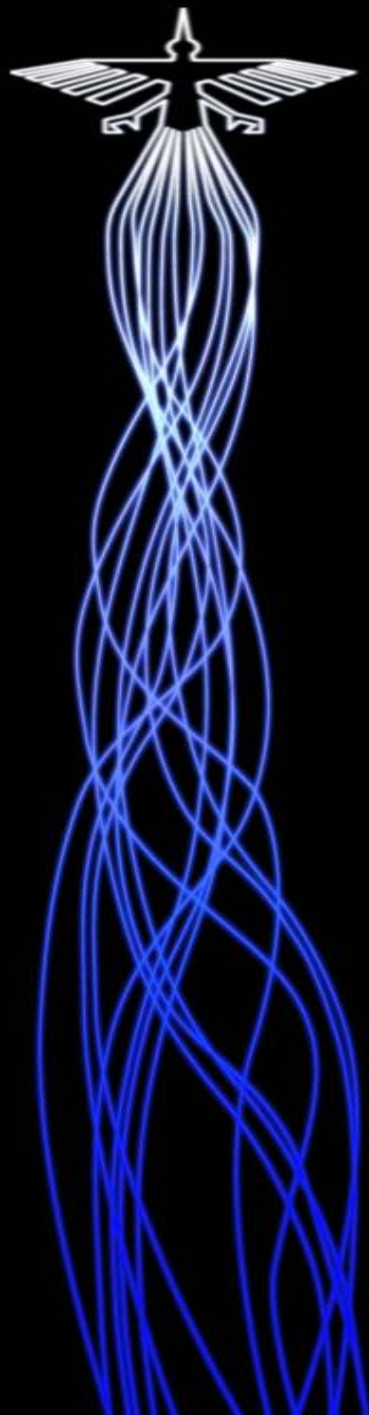
The Other Problem with Education

It is not clear how to best deliver that knowledge to all of the relevant constituencies.

Educational institutions are very diverse

Computer education programs are also very diverse and focused at all levels from CCs to Doctoral work

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



The Other Problem with Education

Nobody in our current classrooms has any more knowledge about the topic than the students they teach.

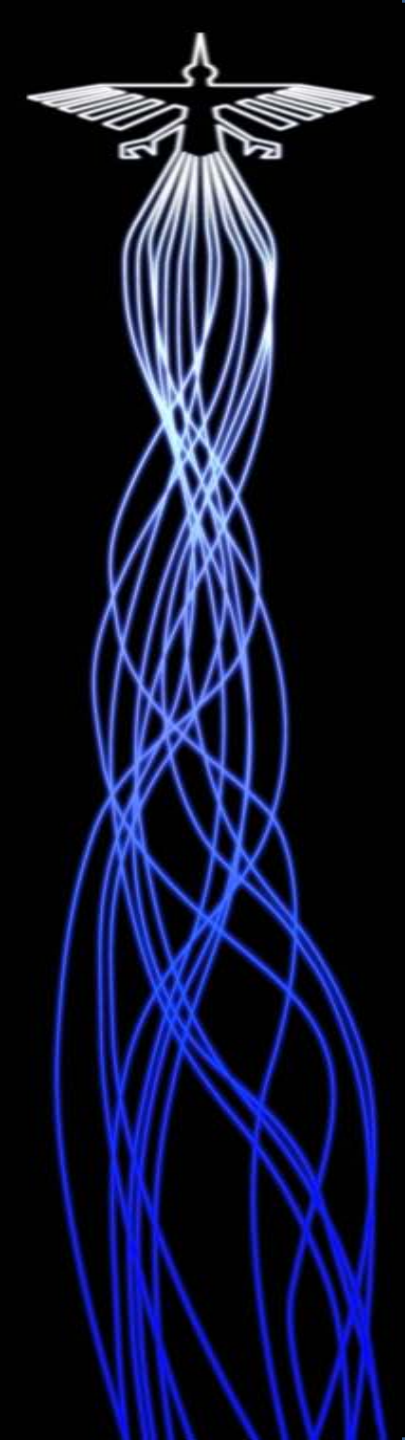
Most senior faculty got their degrees in the 1970s and 1980s

Very few PhDs have been produced heretofore

Teachers would need 42 hours of things to talk about to offer a new subject

Instructional materials are just coming out on the topic

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



The Last Problem with Education

SwA – does not have an accrediting body or national society to underwrite its validity

Programs of study are validated by adherence to commonly accepted models for the discipline

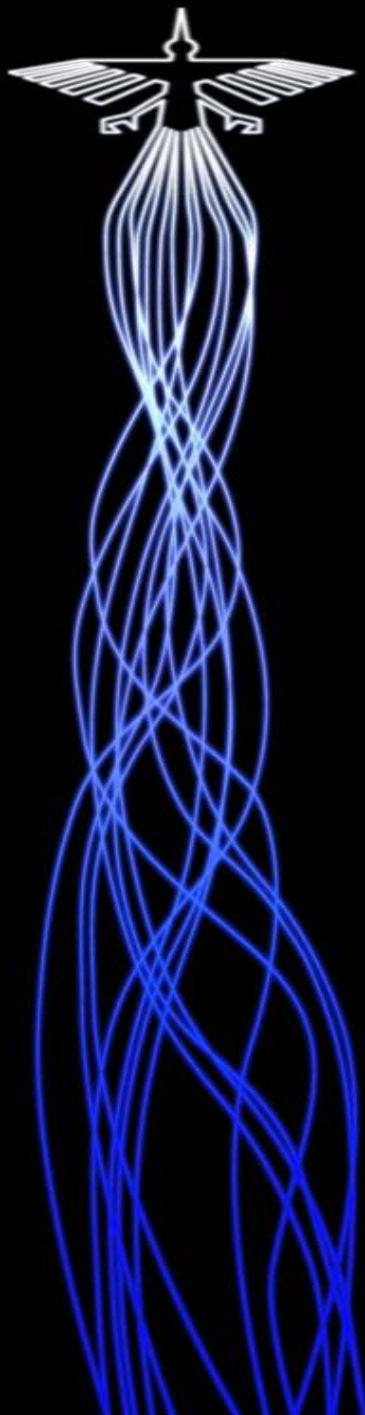
That is – you cannot legitimately call yourself program of study if your curriculum does not comply with the recommendations of:

-Computer Science (ACM) – CS 2001/ CS 2008
-Software Engineering (IEEE) – SE 2004
-Information Systems (AIS) – IS 2002/MSIS 2006

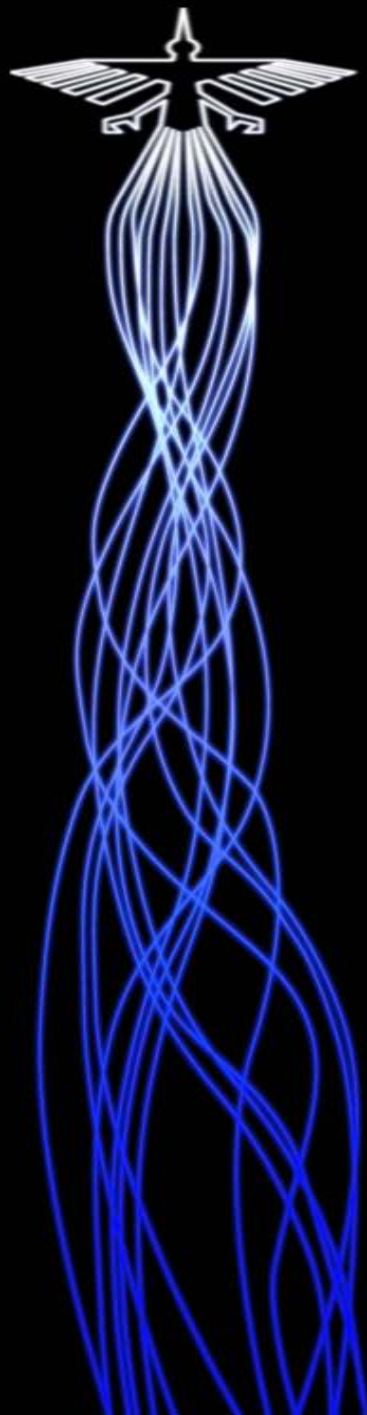
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES

From the Top – Initiative One: The MSwA

- The first initiative focuses on the development of a master of software assurance reference curriculum MSwA
  - This effort was conducted under the leadership of the Software Engineering Institute, in support of DHS's National Cyber Security Division.
- This project specifies a set of topics and the perquisite knowledge and requirements needed to ensure a properly educated software assurance professional.
  - This initiative identifies the topics that effective software assurance professionals must be proficient in and structures that set of topics into a comprehensive curriculum.



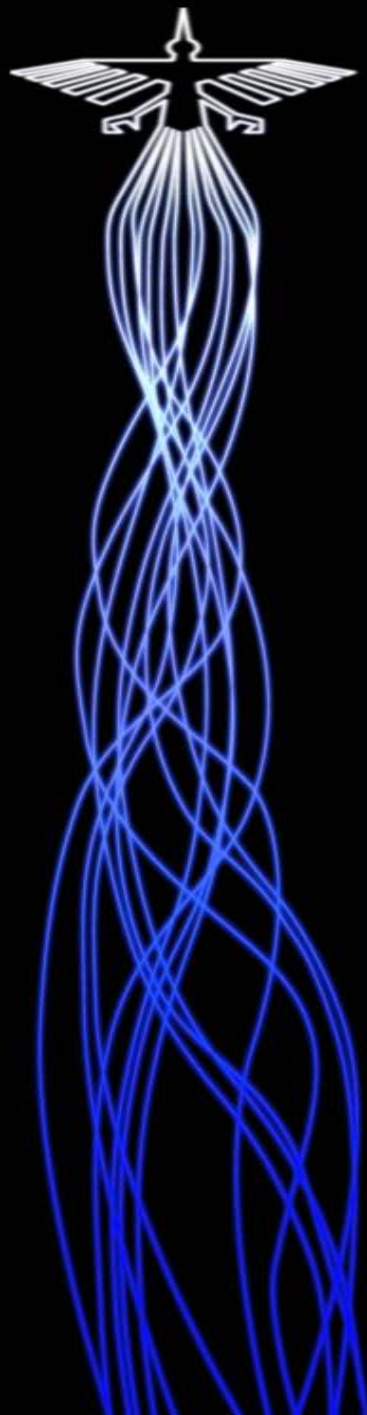
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



From the Top – Initiative One: The MSwA

- That curriculum contains just those key knowledge elements required to produce a well educated practitioner.
  - **Assurance Across Life Cycles** - Graduates will have the ability to incorporate assurance technologies and methods into life-cycle processes and development models for new or evolutionary system development, and for system or service acquisition.
  - **Risk Management** - Graduates will have the ability to perform risk analysis and tradeoff assessment, and to prioritize security measures.
  - **Assurance Assessment** - Graduates will have the ability to analyze and validate the effectiveness of assurance operations and create auditable evidence of security measures.
  - **Assurance Management** - Graduates will have the ability to make a business case for software assurance, lead assurance efforts, understand standards, comply with regulations, plan for business continuity, and keep

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES

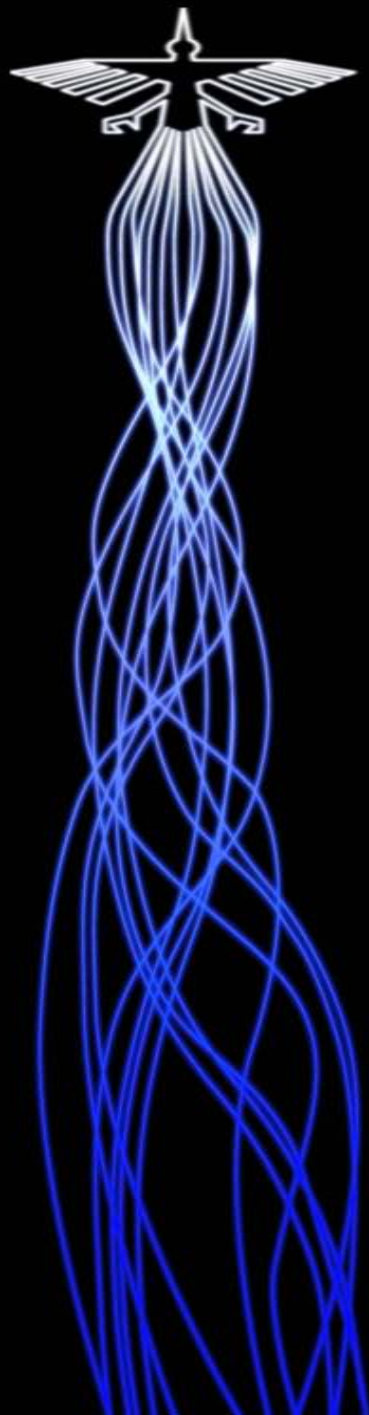


From the Top – Initiative One: The MSwA

- **System Security Assurance** - Graduates will have the ability to incorporate effective security technologies and methods into new and existing systems.
- **System Functionality Assurance** - Graduates will have the ability to verify new and existing software system functionality for conformance to requirements and to help reveal malicious content.
- **System Operational Assurance** - Graduates will have the ability to monitor and assess system operational security and respond to new threats.

- The curriculum development team included technical staff from the SEI and faculty from a number of universities

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES

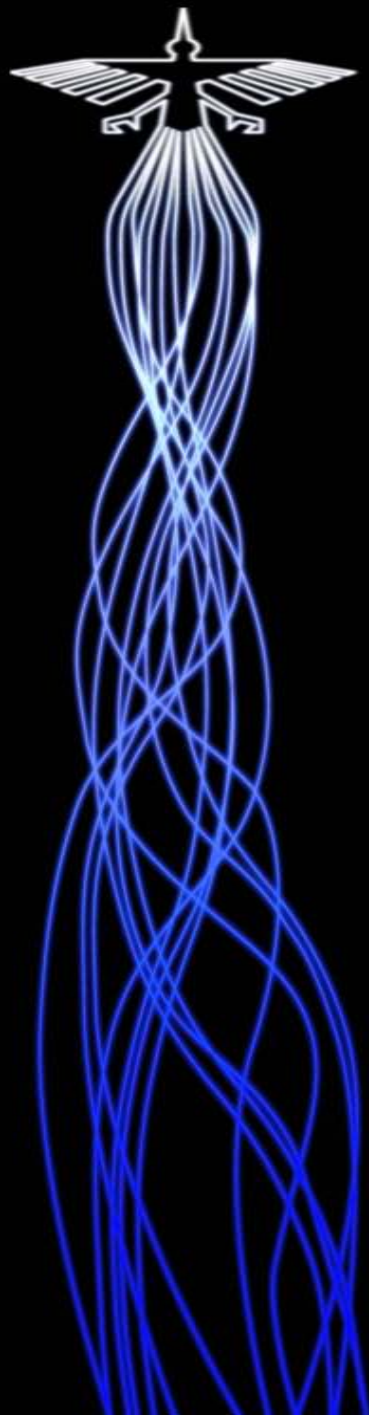


From the Top – Initiative One: The MSwA

- The final report contains the reference curriculum along with the guidelines used by that team in developing:
  - the curriculum
  - Prerequisites
  - proposed outcomes
  - when a student graduates
  - the curriculum architecture
  - the proposed curricular body of knowledge
  - implementation guidelines for the curriculum
  - and a glossary of terms.

- A number of existing artifacts, including the CBK and the recent GSwERC are inputs to the project.

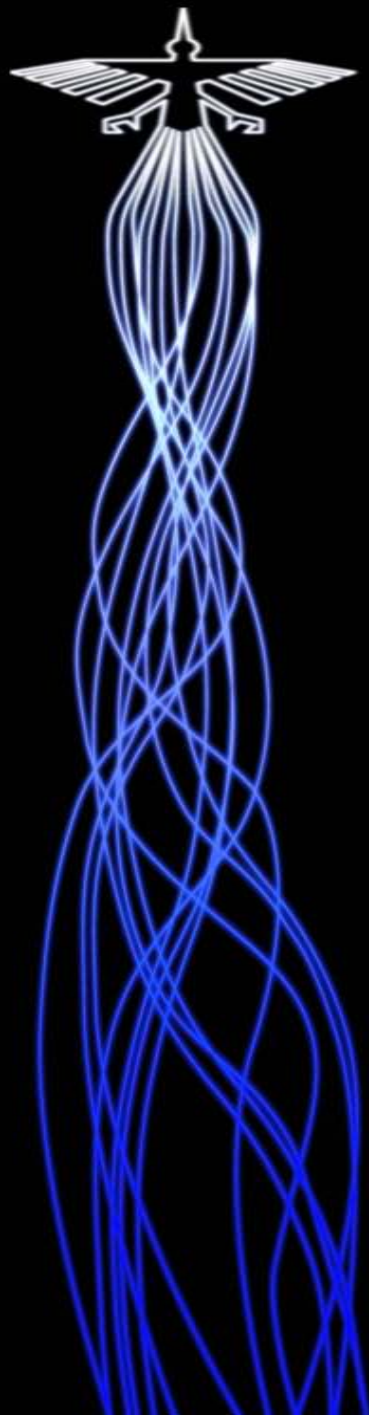
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



From the Top – Initiative One: The MSwA

- The curriculum also includes a detailed list of knowledge units, and corresponding Bloom's taxonomy levels
  - That was provided in order to ensure a sufficient level of understanding for the purposes of implementing
- This curriculum has been approved by IEEE and ACM
- This curriculum is available at http://www.cert.org/mswa/

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Next Level– Implementing the MSwA

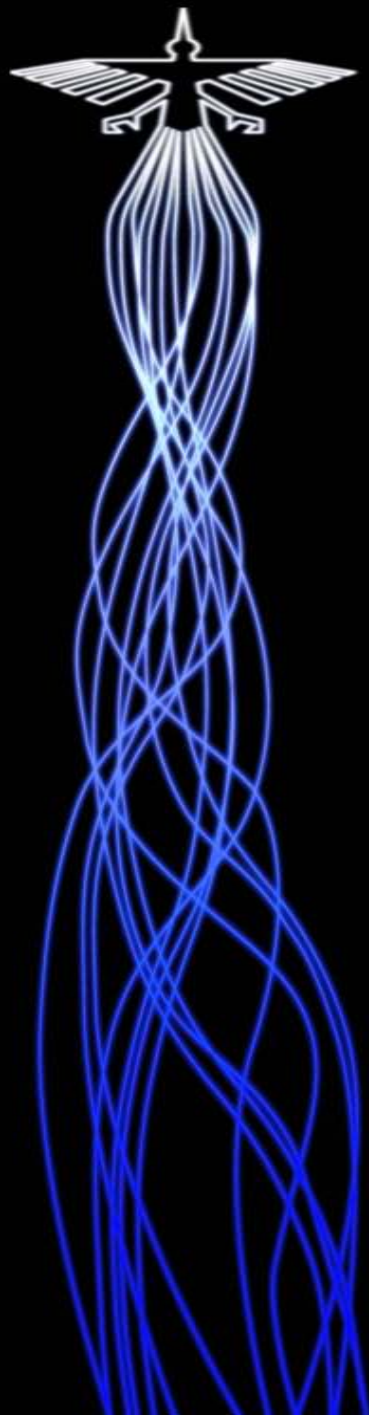
- Establishment of a new degree program is a very ambitious undertaking.
- As a consequence, the SEI project anticipated that some universities would elect to establish tracks or specializations in software assurance within existing master's degree programs rather than establishing a separate new degree program.
- As a proof of concept, Stevens Institute of Technology has implemented the reference curriculum that was just described

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES

Next Level– Implementing the MSwA

- This is done as two tracks within their Master of Science in Software Engineering program.
  - In addition, they are offering two graduate certificates based on the courses in that curriculum.
- As was just mentioned, it is easier for universities to establish tracks within existing programs than it is to create entire new programs.
- In this case Stevens already had three relevant graduate programs: software engineering, system security engineering, and computer science

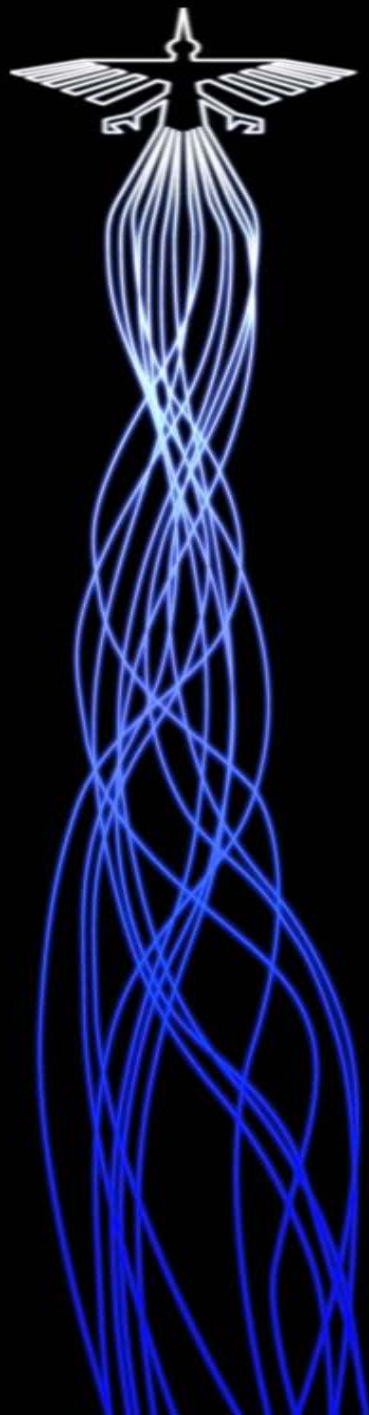
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Next Level– Implementing the MSwA

- Each of these programs contained some of the material of the reference curriculum for software assurance.
- In addition, the software engineering faculty reached the conclusion that every Steven's software engineering student should know how to engineer and build trustworthy, that is,, safe, secure, and reliable systems.
- Since security needs to be addressed throughout the software development lifecycle, they chose to integrate the software assurance curriculum into the existing software engineering curriculum, to the maximum extent possible.

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Next Level– Implementing the MSwA

- There were several issues with utilizing this strategy to implement the curriculum.
  - First, the majority of the software engineering faculty was not particularly strong in security, so even though they were extremely motivated to change, and they were experienced faculty, there was considerable effort required to learn, fully understand and prioritize the content. Not to mention the effort that was needed to create the new material.
- Second, the existing courses were already content rich.
  - Because there was already existing content in those courses, effort was required to decide which material to remove so that secure software knowledge could be added.

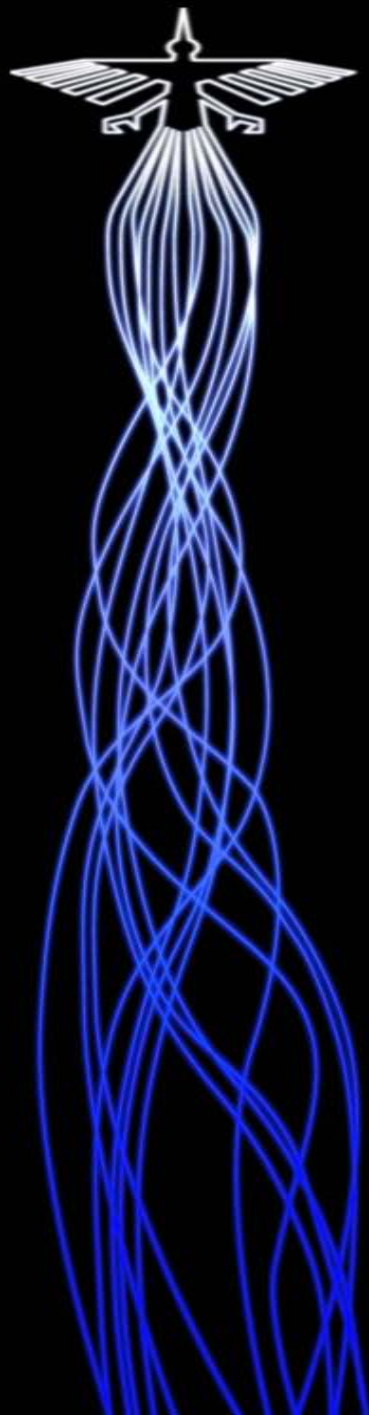
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES

Next Level– Implementing the MSwA

- Third, there wasn't a simple mapping from the recommendations of the reference curriculum to the existing courses.

- Finally, there were significant overlaps between parts of the software assurance curriculum and courses in the systems security engineering program.
  - Some additional material was added to these courses to support the curriculum, and they became part of the software assurance tracks as well.

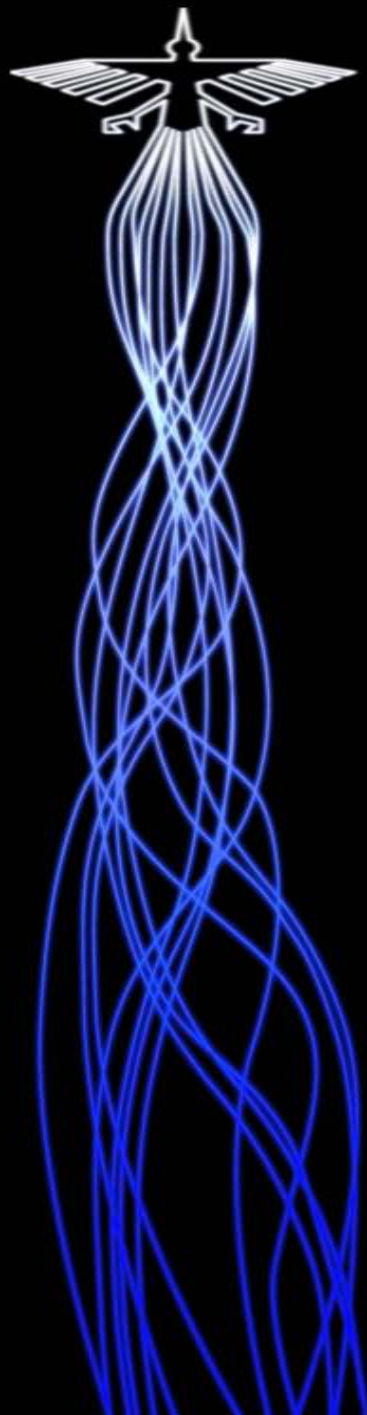
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Next Level– Implementing the MSwA

- The resulting software assurance program at Stevens consists of two new, multi-disciplinary software assurance tracks within software engineering
- One is intended for students interested in careers in software development of trusted systems
- One is intended for students interested in careers in acquisition and management of trusted systems.
- Both tracks share the same six core courses in software engineering.

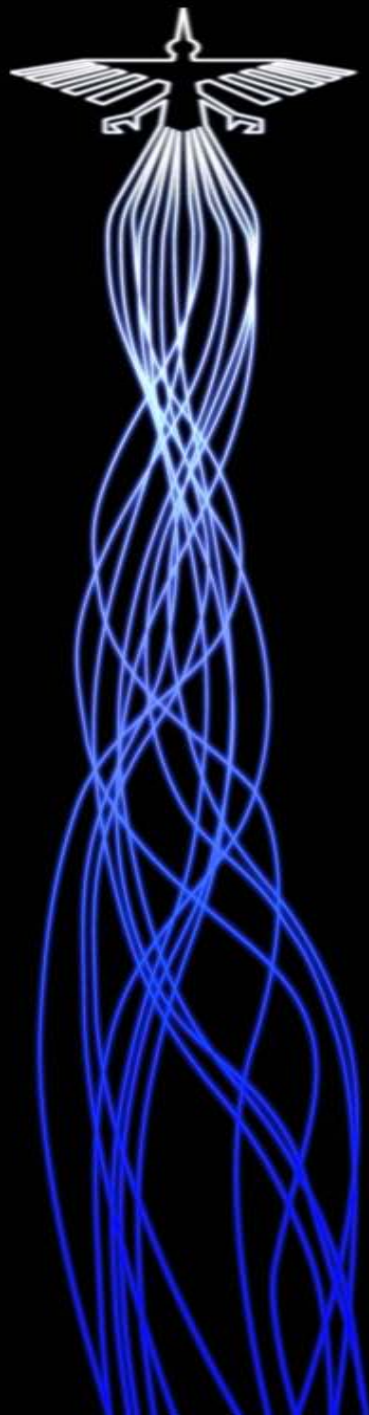
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Next Level– Implementing the MSwA

- Students who already have a graduate degree, or who are not yet ready to enroll in a full master's level program, may take courses to earn a graduate certificate.
- There are 2 certificates, one for students interested in software development of trusted systems
- And one for students interested in acquisition and management of trusted systems.
- Schools interested in adopting similar programs will be given help in establishing and implementing their programs.

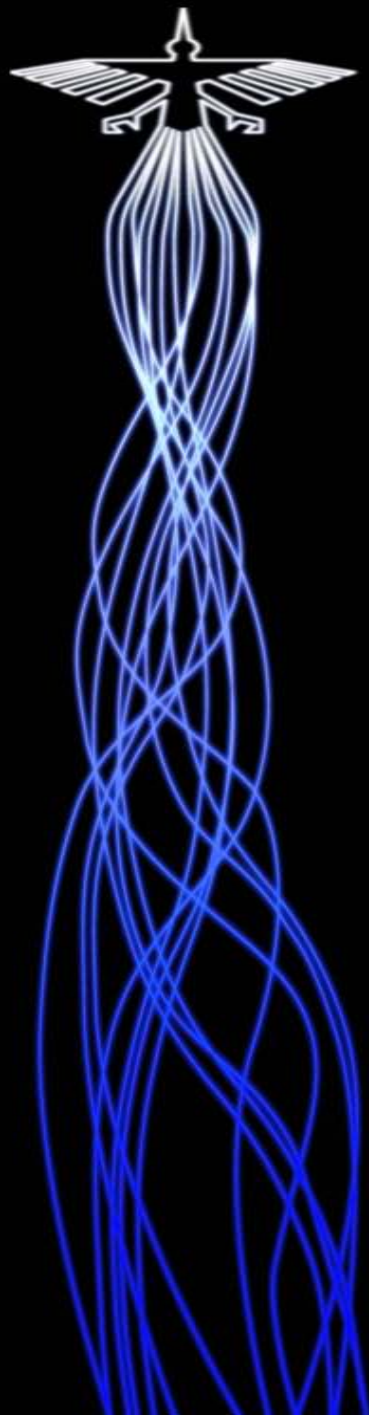
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Initiative Three: Supporting the Teaching Process

- Logically, the first step in integrating new knowledge into a conventional learning setting is to identify, relate and catalogue what is presently out there.
- That is the purpose of a two-year project funded by the Department of Defense (DoD) and conducted at the University of Detroit Mercy.
- This project attempted to identify and document any knowledge, from any source, that could be related to the assurance of software.

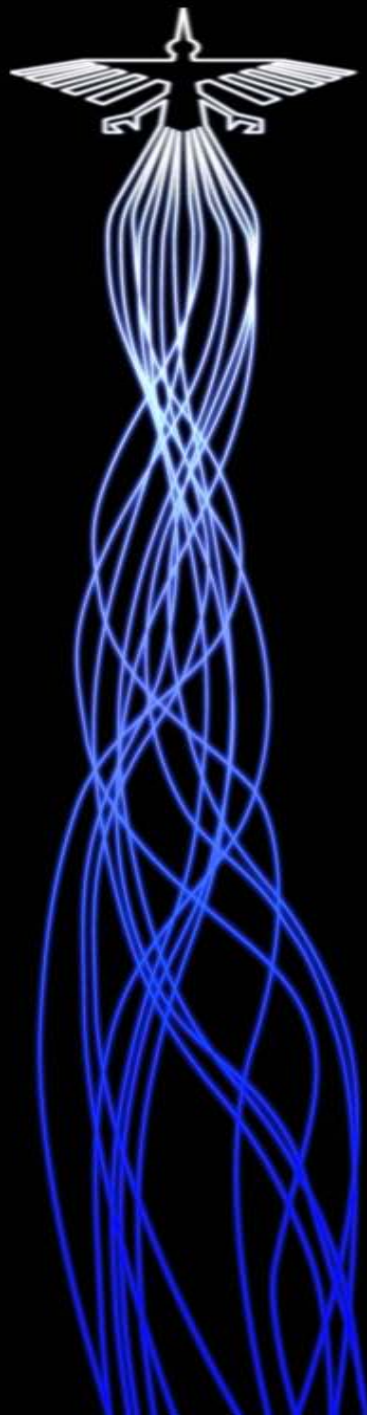
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Initiative Three: Supporting the Teaching Process

- The knowledge base that was the product of this year long study documented and categorized all commonly accepted practices, principles, methodologies and tools for software assurance.
- In addition, the knowledge base incorporates as many lifecycle methodologies and tools for assuring software as could be identified.
- This knowledge base is fully web accessible to anybody who wishes to use it

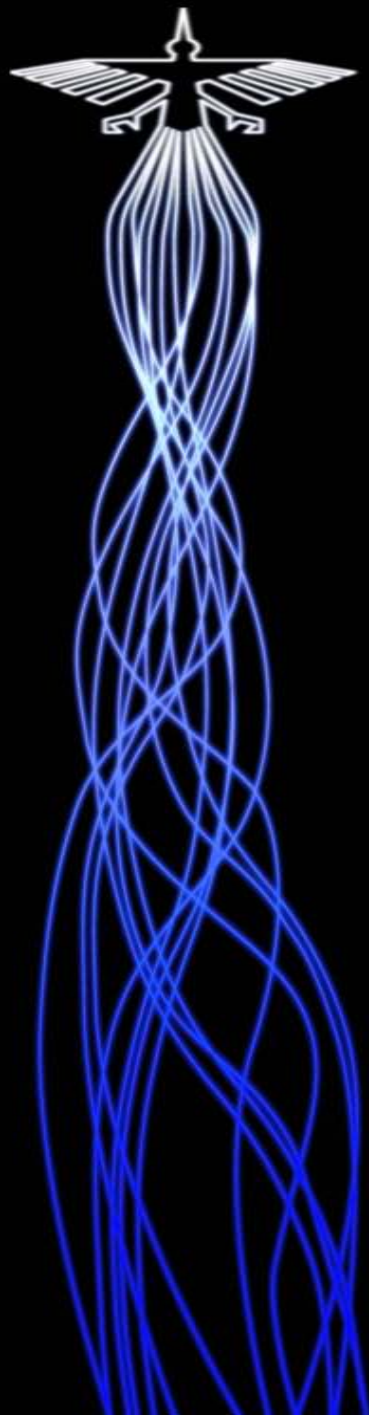
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Initiative Three: Supporting the Teaching Process

- Nevertheless, the actual purpose this initiative was to ensure the teaching of secure software topics in all suitable education, training and awareness settings.
- In support of that goal, the project then packaged the contents of the knowledge base into discrete learning modules.
- These modules are meant to facilitate the efficient transfer of software assurance knowledge into all relevant teaching and learning settings.
  - They are appropriate for traditional graduate and undergraduate, community college and even high school education, as well as training and awareness applications.

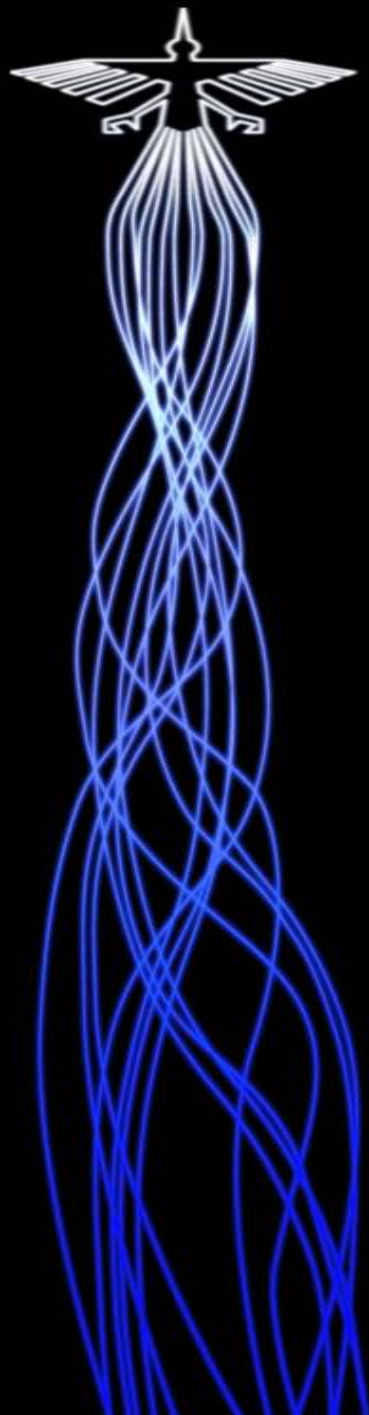
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Initiative Three: Supporting the Teaching Process

- The modules are intended to be standalone teaching artifacts capable of conveying all of the requisite know-how for a discrete topic.
- Each module conveys a logical element of software assurance practice.
- The entire collection of these modules is mapped to the body of knowledge contained in the knowledge base.

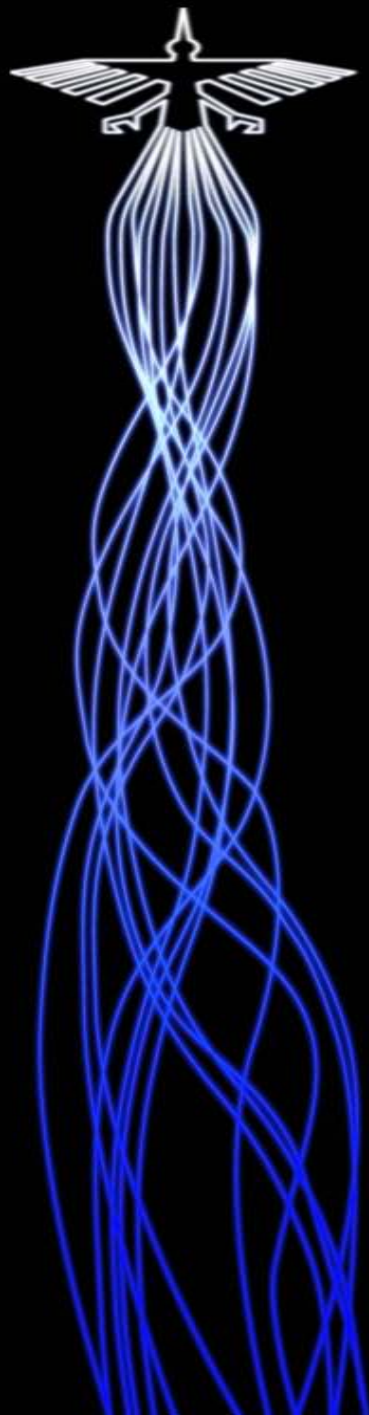
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Initiative Three: Supporting the Teaching Process

- These modules were divided into three topic areas, which were based on the CBK.
- These topics were 1) development of secure code, 2) secure sustainment of code and 3) acquisition of secure code.
- To ensure that these modules would be free standing for any application, the development of secure code was further decomposed into
  - risk understanding and threat modeling
  - a series of modules devoted to secure coding methods and techniques.

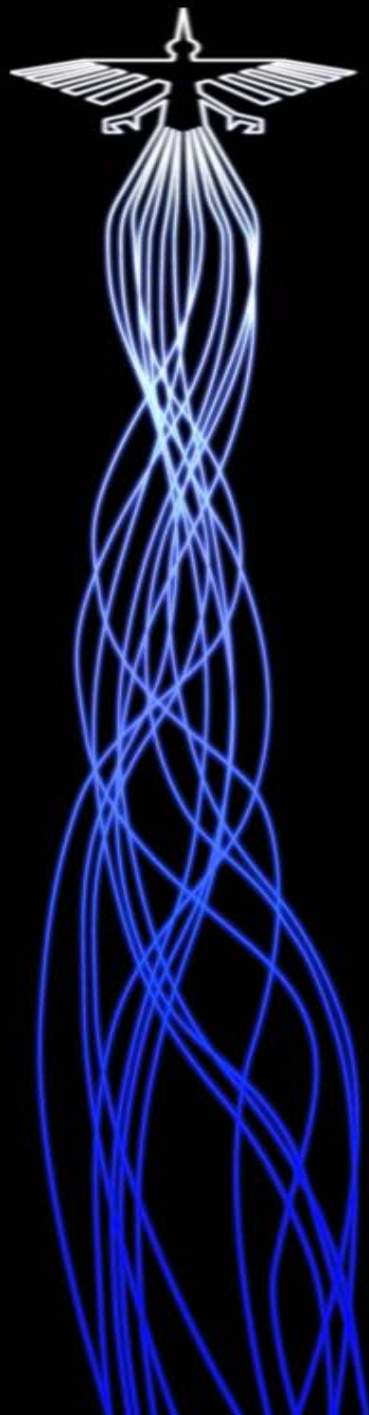
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Initiative Three: Supporting the Teaching Process

- The sustainment process was further decomposed into
  - ethical hacking, as operational testing for vulnerability identification,
  - environmental monitoring and reporting
  - risk analysis
  - Authorization
  - change control
  - patch management.
- Finally, secure acquisition was decomposed into
  - acquisition initiation
  - secure specification
  - contract formulation and delivery management.

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Initiative Three: Supporting the Teaching Process

- Each of the actual teaching modules incorporates a set of conventional learning support artifacts, which are easily recognizable to traditional educators.

- Every module includes
  - a table of learning specifications
  - presentation slides for each concept contained in the module
  - A model evaluation process
  - any relevant web-enabled supporting material
  - Videos
  - a model lesson plan

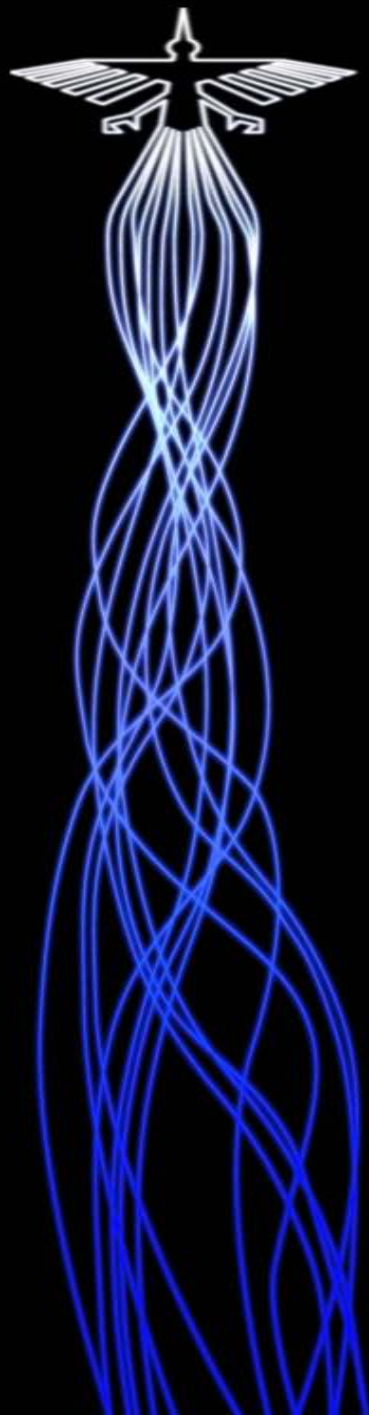
CENTER for CYBER SECURITY and INTELLIGENCE STUDIES

Initiative Three: Supporting the Teaching Process

- Every module also incorporates a validated set of teaching tools.
  - These tools are optimized to ensure the maximum knowledge transfer for all potential teaching settings.

- Finally , the project packaged all of this content onto an innovative knowledge transfer device.
  - That device is based on an i-pad.
  - It allows the project to disseminate the targeted courseware artifacts to classroom teachers, who range from higher education down to K-12.
  - The device is called the Software Assurance Mobile Instructional [device], or SAMI.

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES



Initiative Three: Supporting the Teaching Process

- SAMI bundles all of the knowledge developed by this project into a single portable platform
- Which in addition to providing carry-around storage for all required instructional materials… It also allows internet access to the contents of the software assurance repository.
- The advantage of SAMI is that it provides conventional teachers with all of the knowledge and courseware that they will need to begin to immediately teach topics that might not have been part of their own background, or preparation.

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES

Thank You for Your Attention

Dan Shoemaker - shoemadp@udmercy.edu

Professor and Senior Research Scientist

Center for Cybersecurity and Intelligence Studies

University of Detroit Mercy