WHEREAS the National Science Foundation (NSF) has funded a program that will increase the number of qualified professionals in the field of information assurance and systems security by creating systems security training centers; and

WHEREAS the University of Illinois at Springfield is one of seven partner institutions in one such center, the Center for Systems Security and Information Assurance (CSSIA), based at Moraine Valley Community College; and

WHEREAS the Computer Science Program proposes to use the CSSIA training program as the basis for offering a 16 credit hour graduate certificate in Systems Security and a 16 credit hour graduate certificate in Information Assurance;

BE IT THEREFORE RESOLVED that the Campus Senate of the University of Illinois at Springfield approves the graduate certificate in Systems Security and the graduate certificate in Information Assurance.
A. Introduction

With the global reliance on computers and computer networks in government, business, and education, the security of computer-based information has become a leading world-wide concern. In recognition of this fact, the National Science Foundation (NSF) has funded a program that will increase the number of qualified professionals in the field of information assurance and systems security by creating systems security training centers. The University of Illinois at Springfield is one of seven partner institutions in one such center, the Center for Systems Security and Information Assurance (CSSIA), based at Moraine Valley Community College.

CSSIA will offer advanced training in information assurance and systems security to college faculty members, who, in turn, will be able to train their students in the fundamentals of information assurance and systems security.

UIS proposes to use the CSSIA training program as the basis for offering a Graduate Certificate in Systems Security

The CSSIA training will be complemented by graduate-level learning activities and projects in courses offered through the UIS Computer Science program. The intent of the principal investigators of the CSSIA grant is that the proposed UIS graduate certificate program will serve as a model for other universities that plan to award graduate certificates to CSSIA participants.

UIS is the only four-year university among the seven institutions that form CSSIA and CSSIA is the first NSF funded regional center to include both community colleges and universities. UIS was selected to participate in the project based on its success as a Regional Cisco Networking Academy. UIS was a pioneer in developing and offering graduate credit for educators who completed the professional development classes required to teach in the regional and local academies. Dr. Ted Mims of UIS participated in development of the grant proposal and was invited to make a presentation to the NSF staff members who evaluated the CSSIA proposal. The NSF staff members approved including funding for UIS to develop a plan for offering a graduate certificate for the college faculty participating in the classes that are offered as part of the CSSIA project.

UIS’ involvement with the CSSIA project led to the inclusion of funding in the CSSIA grant to cover a portion of the tuition for project participants who wish to receive graduate credit and graduate certificates upon completion of the project-related courses.
B. Purpose of Graduate Certificate in Systems Security

1. Objectives for the Certificate in Systems Security

As a result of taking the graduate Certificate in Systems Security, students will develop

- A working knowledge of the core concepts that will be covered in a security awareness course
- An advanced working knowledge of the core concepts that will be covered in a two course sequence on network security
- An advanced working knowledge of the core concepts that will be covered in a course on wireless networks
- An advanced working knowledge of the core concepts that will be covered in a capstone course on network security design

2. Specific learning outcomes for the objectives of the Certificate in Systems Security

Learning outcomes associated with each of the objectives are delineated below. Because all of the students in the graduate certificate program will be college teachers, the outcomes are expressed in terms of teachers’ learning outcomes to avoid confusion when referring to the teachers’ students:

- Teachers will be able to present lectures including electronic presentations on topics including legal aspects of information privacy, security awareness, and roles and responsibilities of end users. The teachers will develop case studies and laboratory exercises that demonstrate safe and unsafe privacy and security practices for use in delivering the class to their students.

- Teachers will be able to present lectures including electronic presentations on topics including the basics of network security policy design and management, firewalls, virtual private networks and encryption technologies. The teachers will develop case studies and laboratory exercises that demonstrate the proper design and manage of networks that include firewalls, virtual private networks and encryption technologies for use in delivering the network security classes to their students.

- Teachers will be able to present lectures including electronic presentations on topics including designing, planning, implementing and troubleshooting wireless networks. The teachers will develop case studies and laboratory exercises that demonstrate the proper techniques for designing, implementing, and trouble shooting techniques for wireless networks for use in delivering the class to their students.

- Teachers will be able to manage group projects that involve their students in a capstone course on network security design. The teachers will develop case studies and laboratory exercises that are designed to challenge their students to develop a secure system from the ground up. The teachers will participate in laboratory exercises similar to the ones they will have their students complete. The teachers will experience working on a team project building a secure system and they will also get the opportunity to work on a team project competition that
requires them to a secure system and attempt an intrusion on a secured system.

- Teachers will develop a portfolio of the course work they complete as part of the graduate certificate. They will be able to document their experiences with the certificate program and how they plan to incorporate the topics covered in the certificate program into the courses they teach. The electronic portfolio will be similar to documentation that students participating in UIS’ Applied Study Term (AST) and Graduate Public Service Internship (GPSI) programs are required to maintain. Completion of the portfolio will serve as a closure exercise for the graduate certificate program.

C. Target audiences

As noted above, the purpose of establishing the Graduate Certificate in Systems Security is to provide college faculty with an option to earn graduate credit for professional development classes that are being taught as part of the NSF-funded Center for Systems Security and Information Assurance (CSSIA). Therefore, at this time, the target audience for the proposed graduate certificate is restricted to college faculty participating in the NSF-funded CSSIA project. Interested CSSIA participants will be eligible to apply for admission to the graduate certificate program. Participants selected to participate in the graduate certificate program will hold a bachelor’s degree and will have prior experience teaching computer science or technology courses. It is anticipated that many of the participants will hold professional certifications in the fields of networking and/or security.

D. Proposed curriculum

The curriculum for the Certificate in Systems Security will be based on topics covered in the following classes: Security Awareness for teachers, Network Security I for teachers, Network Security II for teachers, Emerging Technologies Wireless Networks for teachers, Network Security Design for teachers, and Graduate Certificate Portfolio. The class participants will be required to participate in online laboratory sessions. In addition to the lecture and laboratory hours, to earn UIS credit participants will be required to develop electronic instructional modules, participate in online discussions via Blackboard, complete an online assessment to determine their level of mastery of the course materials, and maintain an electronic portfolio. The participants who successfully complete all the classes and all required work for the Certificate in Systems Security will earn 16 hours of graduate credit.

A list of courses that will make up the curriculum for the graduate Certificate is presented in Appendix A. The curriculum for these courses is being developed collaboratively by the principal investigators of the CSSIA grant. Dr. Ted Mims has been directly involved in the course development process. He reviewed the content of each course and has determined that the content is appropriate for graduate credit at UIS.

E. Relation to degree programs

The UIS MS in computer science is focused on introducing students to advanced theoretical concepts in computer science, primarily in the area of software development. In contrast, the graduate certificate is focused on preparing students to develop curriculum and teach courses in a single area within the discipline of computer science not emphasized in the master’s degree curriculum, systems security.
Students in the graduate certificate program would be eligible to apply for admission to the UIS MS in computer science. Assuming they met all prerequisites and were fully admitted to the master’s program, participants of the graduate certificate program choosing to pursue the master’s degree would be permitted to petition to count a maximum of 12 hrs of the certificate toward the master’s degree. At the present time, however, movement of students from the certificate program to the master’s degree will be quite limited. While the graduate certificate will be offered online and will attract students from across the country, the current MS in computer science is offered only on-campus.

Based on experience with the graduate certificate, in the future the Computer Science Department at UIS may seek permission to add an online master’s degree in information assurance and systems security or modify the current master’s degree to include an online concentration in information assurance and systems security.

F. Occupational and/or student demand

The online Graduate Certificate in Systems Security is a component of a NSF grant. The grant funded the Center for Systems Security and Information Assurance (CSSIA). An abstract describing the grant is posted at http://www.uis.edu/~mims/security/NSFCSSIAAward.pdf. During the four year project, it is anticipated that at least 500 college faculty will be trained as part of this grant with a majority of the faculty participating in a graduate certificate program. In turn, it is anticipated that several thousand college students will take classes from these newly-trained college faculty. Dr. Ted Mims is a co-principal investigator for the grant and has the responsibility for coordinating the development of a graduate certificate model for universities that plan to offer graduate credit for the college faculty participants.

G. Staffing and resource requirements

1. Staffing

Erich Spengler, the lead principal investigator for the CSSIA grant, will be responsible for selecting qualified instructors to teach the classes that the college faculty will be taking. Funding from the grant will cover the stipends paid to the CSSIA staff that will teach the classes. These teachers will hold industry certifications and/or master’s degrees. UIS will not be required to pay the CSSIA staff that will be teaching the classes at remote sites.

Dr. Ted Mims is one of the principal investigators for the NSF grant for CSSIA. His primary responsibility related to the grant is to develop a model of a graduate certificate option for the college teachers being trained in the classes offered by CSSIA. This model will be shared with other institutions. He will be the instructor of record for UIS courses associated with the CSSIA training module; will be responsible for evaluating the participants’ work; and, in consultation with the CSSIA staff, will award grades for each of the courses.

2. Resources

The only resource required to offer the graduate certificate at UIS is the compensation for Dr. Mims. The NSF grant will provide Dr. Mims a stipend each of the four years of the grant as the principal investigator responsible for
coordinating the awarding of graduate credit and the graduate certificate to the project participants. It is anticipated that Dr. Mims will receive the standard one month’s salary as the UIS teacher of record for the graduate certificate classes.

No additional staffing or resources will be required for this proposed graduate certificate program.

H. Administrative issues

1. Responsible Administrative Unit

The Computer Science Department will be the administrative unit responsible for administering the Graduate Certificate in Systems Security.

2. Admissions

a) Eligibility

Participants must be approved by their institution to participate in the NSF funded Center for Systems Security and Information Assurance (CSSIA) training.


Courses for the certificate will be offered by the Center for Systems Security and Information Assurance (CSSIA).

The participants in the certificate program must have earned a bachelor’s degree.
b) Admissions process

Participants will complete the standard UIS graduate application forms and supply official transcripts from schools from which they earned bachelor’s and graduate credit.

The UIS admissions office will collect the application form and transcripts and forward them to the Computer Science Department for evaluation.

The applications will be reviewed by the Computer Science Department’s graduate student coordinator.

After the coordinator validates that all required transcripts have been received and that the students have been approved to participate in the CSSIA training, they will be admitted to the graduate certificate program.

3. Advising

Dr. Ted Mims will be the assigned advisor for the participants. If the number of participants grows to a number that he cannot adequately advise, additional faculty will be requested to assist in the advising of these students.

4. Tracking

The Banner student information system will be used to monitor and track the progress of the students completing the degree certificate program. Formal written reports will be prepared and submitted to the National Science Foundation and to the grant’s evaluation team.
Certificate in Systems Security Required Courses 16 Credit Hrs.

1. **CSC 526 Security Awareness for Teachers 1 Credit Hr**

   **Course Description**
   This short course is design to provide an overview of the consequence of information assurance and privacy for the user of information systems. The course provides a practical consideration of all aspects of network security. Course topics include legal aspects of information privacy, security awareness, and roles and responsibilities of end users. The course will examine several case studies that will illustrate the types of problems that can occur if good systems security measures are not followed.

2. **CSC 527 Network Security I for Teachers 3 Credit Hrs.**

   **Course Description**
   Introduction to Network Security course focusing on the overall security processes with particular emphasis on security policy design & management. This course will also provide a survey of security technologies, products & solutions. The course will also include hands-on exercises focusing on firewall design, installation, configuration, & maintenance and AAA implementation using routers and firewalls. Virtual Private Networks will also be introduced using routers and firewalls.

3. **CSC 528 Network Security II for Teachers 3 Credit Hrs.**

   **Course Description**
   This course will provide an introduction to the knowledge and skills needed to describe, configure, verify and manage IPSec features in VPN solutions. The course provides a multi-vendor solution to VPN design. Examination of both VPN client and server products will prepare students to deploy VPN technologies in both site-to-site and client-to-site configurations. The course will survey many of the encryption technologies including: PKI, IPSEC and 3DES. Both digital certificates and certificate authorities are introduced in this course. The course will also emphasize intrusion detection systems, a systematic approach to perimeter security.

4. **CSC 529 Emerging Technologies Wireless Networks for Teachers 3 Credit Hrs.**

   **Course Description**
   This course will provide an introduction to wireless local area networks. Instruction will focus on the design, planning, implementation, operation and troubleshooting of wireless networks. It covers a comprehensive overview of technologies, security, and design best practices with particular emphasis on hands-on skills. The hands-on exercises will focus on:

   - Designing a logical wireless LAN architecture for mobile wireless users in compliance with 802.11 IEEE standards.
   - Demonstrating a working knowledge in WLAN applications as they relate to EM spectrum, radio wave propagation, modulation techniques, and frequency and channel usage in wireless technologies.
   - Installation of in-building and building-to-building wireless LANs with Cisco devices that meet mobility and throughput specifications including the site survey and documentation.
• Performing hardware setup and software configuration of Cisco Aironet APs and antennas for Ethernet/Radio ports, and services.
• Performing hardware setup and software configuration of Cisco Aironet equipment for Ethernet/Radio ports and services specific to the WLAN needs for Access Points, Bridges, Repeater, and Site Survey Client functionality.
• Upgrading and distributing firmware on Cisco wireless products throughout a WLAN.
• Identifying, defining features of, and installing, directional and omni directional antennas in both building-to-building and in-building WLANs.
• Designing and setting up of WLAN security using WEP, Cisco LEAP and 802.1x protocols.

Troubleshooting WLAN performance issues using event loggings, command line utilities, and diagnostic tools.

5. CSC 530 Security Design for Teachers 3 Credit Hrs.

Course Description
This is the capstone design course for the Graduate Certificate in Systems Security. This course will emphasize a group approach to security systems design. Student cohort groups will be required to develop a comprehensive security plan based on British Standard 7799. The plans will include operational policies and procedures. Students are also required to design a secure enterprise network including multi-vendor solutions. They will use hardware and software tools to implement firewalls, email system protection, virtual private networks, directory service single logon, virus protection software, system documentation, system logging, simple network management protocol, and remote monitoring.

6. CSC 531 Security Graduate Portfolio 3 Credit Hrs.

Course Description
Participants in the Graduate Certificate in Systems Security program must complete a comprehensive portfolio. The portfolio will document their experiences with the certificate program and how they plan to incorporate the topics covered in the certificate program into the courses they teach. The portfolio will document how program participants have mastered the material covered in each course. Guidelines for completing the requirement are available at csc.uis.edu/ and should be consulted by the certificate program participants.
B. Introduction

With the global reliance on computers and computer networks in government, business, and education, the security of computer-based information has become a leading world-wide concern. In recognition of this fact, the National Science Foundation (NSF) has funded a program that will increase the number of qualified professionals in the field of information assurance and systems security by creating systems security training centers. The University of Illinois at Springfield is one of seven partner institutions in one such center, the Center for Systems Security and Information Assurance (CSSIA), based at Moraine Valley Community College.

CSSIA will offer advanced training in information assurance and systems security to college faculty members, who, in turn, will be able to train their students in the fundamentals of information assurance and systems security.

UIS proposes to use the CSSIA training program as the basis for offering a Graduate Certificate in Information Assurance.

The CSSIA training will be complemented by graduate-level learning activities and projects in courses offered through the UIS Computer Science program. The intent of the principal investigators of the CSSIA grant is that the proposed UIS graduate certificate program will serve as a model for other universities that plan to award graduate certificates to CSSIA participants.

UIS is the only four-year university among the seven institutions that form CSSIA and CSSIA is the first NSF funded regional center to include both community colleges and universities. UIS was selected to participate in the project based on its success as a Regional Cisco Networking Academy. UIS was a pioneer in developing and offering graduate credit for educators who completed the professional development classes required to teach in the regional and local academies. Dr. Ted Mims of UIS participated in development of the grant proposal and was invited to make a presentation to the NSF staff members who evaluated the CSSIA proposal. The NSF staff members approved including funding for UIS to develop a plan for offering a graduate certificate for the college faculty participating in the classes that are offered as part of the CSSIA project.

UIS’ involvement with the CSSIA project led to the inclusion of funding in the CSSIA grant to cover a portion of the tuition for project participants who wish to receive graduate credit and graduate certificates upon completion of the project-related courses.
B. Purpose of Graduate Certificate in Information Assurance

3. Objectives for the Certificate in Information Assurance

As a result of completing the graduate Certificate in Information Assurance, students will develop

- An advanced working knowledge of the core concepts that will be covered in a two course sequence on information technology security and data assurance
- An advanced working knowledge of the core concepts that will be covered in the course on computer forensics
- An advanced working knowledge of the core concepts that will be covered in a capstone course on data assurance system design.

4. Specific learning outcomes for the objectives of the Certificate in Information Assurance

Learning outcomes associated with each of the objectives are delineated below. Because all of the students in the graduate certificate program will be college teachers, the outcomes are expressed in terms of teachers’ learning outcomes to avoid confusion when referring to the teachers’ students:

- Teachers will be able to present lectures including electronic presentations on topics including policy and practices used to identify the resources at risk to malicious attacks or natural disasters and solutions provided by multiple vendors. The teachers will develop case studies and laboratory exercises that demonstrate proper techniques for identifying vulnerabilities and preventing intrusions for use in delivering the class to their students.

- Teachers will be able to present lectures on computer forensics topics including evidence handling, chain of custody, collection, preservation, identification and recovery of computer data. The teachers will develop case studies and laboratory exercises that demonstrate the correct and legal methods for evidence handling, chain of custody, collection, preservation, identification and recovery of computer data for use in delivering the classes to their students.

- Teachers will be able to manage group projects that involve their students in a capstone course on system design. The teachers will develop case studies and laboratory exercises that are designed to challenge their students to develop a secure system from the ground up. The teachers will participate in laboratory exercises similar to the ones they will have their students complete. The teachers will experience working on a team project securing a system for data collection. They will also have the opportunity to work on a team project that requires them to attempt an intrusion of a secured system and collect data from a system that has been intruded upon.
Teachers will develop a portfolio of the course work they complete as part of the Graduate Certificate in Information Assurance. They will be able to document their experiences with the certificate program and how they plan to incorporate the topics covered in the certificate program into the information assurance courses they teach. The electronic portfolio will be similar to documentation that students participating in UIS’ Applied Study Term (AST) and Graduate Public Service Internship (GPSI) programs are required to maintain. Completion of the portfolio will serve as a closure exercise for the graduate certificate program.

C. Target audiences

As noted above, the purpose of establishing the Graduate Certificates in Information Assurance is to provide college faculty with an option to earn graduate credit for professional development classes that are being taught as part of the NSF-funded Center for Systems Security and Information Assurance (CSSIA). Therefore, at this time, the target audience for the proposed graduate certificate is restricted to college faculty participating in the NSF-funded CSSIA project. Interested CSSIA participants will be eligible apply for admission to the graduate certificate program. Participants selected to participate in the graduate certificate program will hold a bachelor’s degree and will have prior experience teaching computer science or technology courses. It is anticipated that many of the participants will hold professional certifications in the fields of networking and/or security.

D. Proposed curriculum

The curriculum for the Certificate in Information Assurance will be based on topics covered in the following classes: IT Security and Data Assurance I for teachers, IT Security and Data Assurance II for teachers, Computer Forensics for teachers, Data Assurance System Design for teachers, and Graduate Certificate Portfolio. The class participants will be required to participate in online laboratory sessions. In addition to the lecture and laboratory hours, to earn UIS credit participants will be required to develop electronic instructional modules, participate in online discussions via Blackboard, complete an online assessment to determine their level of mastery of the course materials, and maintain an electronic portfolio. The participants who successfully complete all the classes and all required work for the Certificate in Information Assurance will earn 15 hours of graduate credit.

A list of courses that will make up the curriculum for the graduate certificate is presented in Appendix A. The curriculum for these courses is being developed collaboratively by the principal investigators of the CSSIA grant. Dr. Ted Mims has been directly involved in the course development process. He reviewed the content of each course and has determined that the content is appropriate for graduate credit at UIS.

E. Relation to degree programs

The UIS MS in computer science is focused on introducing students to advanced theoretical concepts in computer science, primarily in the area of software development. In contrast, the graduate certificate is focused on preparing students to
develop curriculum and teach courses in a single area within the discipline of computer science not emphasized in the master’s degree curriculum, information assurance.

Students in the graduate certificate programs would be eligible to apply for admission to the UIS MS in computer science. Assuming they met all prerequisites and were fully admitted to the master’s program, participants of the graduate certificate program choosing to pursue the master’s degree would be permitted to petition to count a maximum of 12 hrs of the certificate toward the master’s degree. At the present time, however, movement of students from the certificate program to the master’s degree will be quite limited. While the graduate certificate will be offered online and will attract students from across the country, the current MS in computer science is offered only on-campus.

Based on experience with the graduate certificate, in the future the Computer Science Department at UIS may seek permission to add an online master’s degree in information assurance and systems security or modify the current master’s degree to include an online concentration in information assurance and systems security.

F. Occupational and/or student demand

The online Graduate Certificate in Information Assurance is a component of a NSF grant. The grant funded the Center for Systems Security and Information Assurance (CSSIA). An abstract describing the grant is posted at [http://www.uis.edu/~mims/security/NSFCSSIAAward.pdf](http://www.uis.edu/~mims/security/NSFCSSIAAward.pdf). During the four year project, it is anticipated that at least 500 college faculty will be trained as part of this grant with a majority of the faculty participating in a graduate certificate program. In turn, it is anticipated that several thousand college students will take classes from these newly-trained college faculty. Dr. Ted Mims is a co-principal investigator for the grant and has the responsibility for coordinating the development of a graduate certificate model for universities that plan to offer graduate credit for the college faculty participants.

G. Staffing and resource requirements

5. Staffing

Erich Spengler, the lead principal investigator for the CSSIA grant, will be responsible for selecting qualified instructors to teach the classes that the college faculty will be taking. Funding from the grant will cover the stipends paid to the CSSIA staff that will teach the classes. These teachers will hold industry certifications and/or master’s degrees. UIS will not be required to pay the CSSIA staff that will be teaching the classes at remote sites.

Dr. Ted Mims is one of the principal investigators for the NSF grant for CSSIA. His primary responsibility related to the grant is to develop a model of a graduate certificate option for the college teachers being trained in the classes offered by CSSIA. This model will be shared with other institutions. He will be the instructor of record for UIS courses associated with the CSSIA training module; will be responsible for evaluating the participants’ work; and, in consultation with the CSSIA staff, will award grades for each of the courses.

6. Resources
The only resource required to offer the graduate certificate at UIS is the compensation for Dr. Mims. The NSF grant will provide Dr. Mims a stipend each of the four years of the grant as the principal investigator responsible for coordinating the awarding of graduate credit and the graduate certificate to the project participants. It is anticipated that Dr. Mims will receive the standard one month’s salary as the UIS teacher of record for the graduate certificate classes.

No additional staffing or resources will be required for this proposed graduate certificate program.

H. Administrative issues

3. Responsible Administrative Unit

The Computer Science Department will be the administrative unit responsible for administering the Graduate Certificate in Information Assurance.

4. Admissions

a) Eligibility

Participants must be approved by their institution to participate in the NSF funded Center for Systems Security and Information Assurance (CSSIA) training.

To earn a Graduate Certificate in Information Assurance, the participants must complete fifteen hours of course work. IT Security and Data Assurance I for teachers, IT Security and Data Assurance II for teachers, Computer Forensics for teachers, Data Assurance System Design for teachers, and Graduate Certificate Portfolio are the required courses for this certificate.

Courses for the certificate will be offered by the Center for Systems Security and Information Assurance (CSSIA).

The participants in the certificate program must have earned a bachelor’s degree.
b) Admissions process

Participants will complete the standard UIS graduate application forms and supply official transcripts from schools from which they earned bachelor’s and graduate credit.

The UIS admissions office will collect the application form and transcripts and forward them to the Computer Science Department for evaluation.

The applications will be reviewed by the Computer Science Department’s graduate student coordinator.

After the coordinator validates that all required transcripts have been received and that the students have been approved to participate in the CSSIA training, they will be admitted to the graduate certificate program.

7. Advising

Dr. Ted Mims will be the assigned advisor for the participants. If the number of participants grows to a number that he cannot adequately advise, additional faculty will be requested to assist in the advising of these students.

8. Tracking

The Banner student information system will be used to monitor and track the progress of the students completing the degree certificate program. Formal written reports will be prepared and submitted to the National Science Foundation and to the grant’s evaluation team.
Certificate in Information Assurance Required Courses 15 Credit Hrs.

1. **CSC 521 IT Security and Data Assurance I for Teachers 3 Credit Hrs.**

   **Course Description**
   This course provides a comprehensive view of policy and practices used to identify the resources at risk to malicious attacks or natural disasters. The course will raise questions and give direction in providing answers to what impact such attacks or disasters would result in. The course also provides a survey of viruses and the implementation of effective anti-virus prevention policies. The course will include the use and demonstration of several instruments used to assess and identify vulnerability including penetration analysis, scanners, and probes. The class will also make use of case studies to identify when an institution should look to outside consultants for assessment and vulnerability testing.

2. **CSC 522 IT Security and Data Assurance II Access Control Systems & Methodology for Teachers 3 Credit Hrs.**

   **Course Description**
   This course will provide a comprehensive examination of a multi-vendor approach to access control and management of an enterprise network. The course will examine directory services, file security, single logon solutions and database security. The student is forced to examine a holistic approach to data protection and privacy. The course will introduce the deployment of access management protocols including TACACS+, Radius, and Kerberos. Other topics examined include auditing, and device monitoring using SNMP and RMON.

3. **CSC 523 Computer Forensics for Teachers 3 Credit Hrs.**

   **Course Description**
   This course deals with the preservation, identification, extraction, documentation and interpretation of computer data. Topics covered include evidence handling, chain of custody, collection, preservation, identification and recovery of computer data. Teachers completing this course will be able to:

   - Describe the handling process of a forensic analysis of a hard disk or floppy disk to include:
     - Securing the data without contamination or compromising the integrity
     - Creating a bit stream image of the original data

   - Demonstrate how to acquire evidence while adhering to reasonable practices of:
     - Handling
     - Chain of custody
     - Collection
     - Identification
     - Transportation
     - Storage
     - Documentation of the investigation

   - Describe and demonstrate how to authenticate forensic evidence to include:
     - Documenting the scene using pictures
     - Creating an electronic fingerprint of acquired data using hashing techniques

   - Describe how and why it is necessary to create a copy of evidence data:
- Forensic backups
- Preservation of the original data

- Describe and demonstrate how to recover data in a forensic evaluation of a hard or floppy disk, to include:
  - Slack data
  - Recycle bin
  - Deleted data
  - Unallocated data
  - Swap data

- Describe the physical and logical disk structure:
  - Disk volumes
  - Data area
  - Cluster size
  - FAT entries
  - Slack

- Identify and describe the system boot process:
  - Power on
  - POST
  - RAM check
  - Hard disk check
  - Video check
  - OS loading

4. **CSC 524 Information Assurance System Design and Analysis for Teachers 3 Credit Hrs.**

**Course Description**
This is the capstone design course for the Graduate Certificate in Information Assurance. This course will emphasize a group approach to information assurance system design and data collection. Cohort groups will be required to develop a comprehensive plan for protecting systems against intrusion and for collecting evidence from systems that have been intruded. The plan will include operational policies and procedures. Students are also required to implement the plan using tools including TACACS+, Radius, Kerberos, encryption software, and software tools used in evidence collection.

5. **CSC 525 Information Assurance Graduate Portfolio 3 Credit Hrs.**

**Course Description**
Participants in the Graduate Certificate in the Information Assurance program must complete a comprehensive portfolio. The portfolio will document their experiences with the certificate program and how they plan to incorporate the topics covered in the certificate program into the courses they teach. The portfolio will document how program participants have mastered the material covered in each course. Guidelines for completing the requirement are available at [csc.uis.edu](http://csc.uis.edu) and should be consulted by the certificate program participants.