Program Proposal for a Minor

1. Name of the proposed minor.
   Cyber Security

2. Name of the department(s) involved.
   Electrical and Computer Engineering

3. Name of contact person(s).
   Julie Rursch (jrursch@iastate.edu), Doug Jacobson (dougj@iastate.edu)


   The minor is intended for students studying computer engineering, computer science, software engineering, or management information systems with the goal of enabling them to work in cyber security. The minor consists of a series of lab based courses that are designed to provide students with both the technical background and the hands-on experiences along with the theoretical background to allow them to compete to jobs in cyber security.

5. Need for the proposed minor.

   The need for cyber security professionals is well documented and Iowa State is well positioned to fill the need. ISU has had a graduate degree in security since 2000. Many of our undergrads that are interested in cyber security take two or three of the graduate courses. And while these students are very successful in getting jobs, we have employers that are requesting students with more of a practical background. In addition, typically this option of taking graduate course is only open to computer engineering students. The minor is designed to complement the graduate degree in security and students getting the minor will be prime candidates for the graduate degree.

6. Objectives of the proposed minor including the student learning outcomes and how the learning outcomes will be assessed.
Objectives
The minor in cyber security is designed to prepare students with the technical skills for entry into cybersecurity positions in industry or government agencies.

A few years after graduation, students completing the cyber security minor should be:

a) Contributing to their communities and society in the area of cyber security technology and applications and demonstrate an understanding of contemporary security issues, both technological and societal.
b) Advancing in their careers through application of their knowledge of cyber security
c) Working effectively as team members and demonstrating ethics and responsible behavior
d) Applying cyber security methods and concepts to the general area of their BS degree
e) Continuing their professional development through life-long learning

Learning Outcomes
After earning the minor in cyber security students will

a) demonstrate the ability to apply knowledge of cyber security concepts, tools and technologies to computer systems.
b) understand cyber security risks, threats and countermeasures and apply this understanding to develop cyber defense strategies.
c) demonstrate the ability to design cyber security systems to meet organizational needs within realistic constraints such as economic, environmental, social, and ethical expectations.
d) demonstrate the ability to function on teams.

Assessment
To assess the learning outcomes, we will use CprE 431 and CprE/INFAS 332, selecting specific assignments from each of these courses. CprE/INFAS 332 acts as a capstone course for this minor and provides many opportunities for assessment. In CprE/INFAS 332 small teams of three to eight students build and securely configure their own “corporate” network as part of a cyber defense competition. After spending a month building the “corporate” network, the students are challenged to experience the real world by defending against attackers for eight hours, as well as providing useable systems for end users and reacting to real-time requests for additional services.

We can use two specific assignments from CprE/INFAS 332 to learning outcomes c and d. At the beginning of the course the students report on their role and tasks they plan to undertake during their network build. At the end of the course they report on what roles and responsibilities they undertook throughout the setup and competition. They also look at how the roles and duties changed based upon need and how the students related to each other.
Another assignment in CprE/INFAS 332 assesses learning outcomes a, b, and c. At the end of the course the students write a very structured reflection paper which asks pointed questions about attacks that their networks sustained and how, in retrospect, they could have prevented those attacks from occurring. The students also report on any remediations they were able to take during the competition to mitigate the damage to their network. They also answer questions about the protection of legacy systems and whether any real-time requests which require students be able to evaluate whether the request is good for the company and if it can be securely implemented were a problem for them.

Learning outcomes a and b can be assessed by a lab at the end of the semester in CprE 431 where students are asked to use tools to find vulnerabilities in servers and then provide the remediations needed to avoid being exploited. In a second lab, the students are given the opportunity to exploit a system to understand the complexity of attacks that can occur on a network.

7. Relationship of the minor to other programs at Iowa State University.

There currently are no undergraduate programs in cyber security at Iowa State. In the department of Electrical and Computer Engineering students studying computer engineering can currently take several graduate courses in cyber security. There are several interdisciplinary graduate degrees in Information Assurance (MS, ME, and Certificate). There is no overlap between the proposed minor and the current graduate degrees.

8. Relationship of the minor to the strategic plans of the university, of the college, and of department or program.

Cyber security is one of the strategic areas in the College of Engineering and in the Department of Electrical and Computer Engineering. Cyber security fits into the strategic plan of the university by educating students into a field with a strong employer demand.

9. Comparison of the proposed minor with similar programs at other universities, including the Regent’s universities.

No other university in the area (including the Regent’s universities) have a minor in cyber security. The closest known school with any focus in cyber security is the University of Nebraska Omaha.
10. Program requirements and procedures, including:

The table below shows the courses used in the minor: (notes students take 332 three times). The courses are divided into three categories; Core courses (9 credits), Capstone experience (3 credits), Elective courses (3 credits). As of now we have only two elective courses, but as the minor matures we anticipate adding additional courses.

<table>
<thead>
<tr>
<th>Course</th>
<th>Credits</th>
<th>Title</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Core Courses (9 credits)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CprE 231</td>
<td>3</td>
<td>Cyber security concepts and tools</td>
<td>New</td>
</tr>
<tr>
<td>Com S 252 or CprE 308 or Com S 352</td>
<td>3</td>
<td>Linux OS Essentials</td>
<td>Existing</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Operating systems principles and practice</td>
<td>Existing</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Introduction to Operating systems</td>
<td>Existing</td>
</tr>
<tr>
<td>CprE 431</td>
<td>3</td>
<td>Introduction to computer security</td>
<td>Existing</td>
</tr>
<tr>
<td><strong>Capstone (3 credits)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFAS 332</td>
<td>1 (3)</td>
<td>Cyber defense competitions</td>
<td>Existing</td>
</tr>
<tr>
<td><strong>Elective (3 credits) [more courses to be added later]</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CprE 430</td>
<td>3</td>
<td>Introduction to network security</td>
<td>Existing (new dual listing)</td>
</tr>
<tr>
<td>Com S 412</td>
<td>3</td>
<td>Formal Methods in Software Engineering</td>
<td>Existing</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>15</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a. prerequisites for prospective students;

The minor is intended for students who are studying in a computer related field (computer engineering, computer science, software engineering, management information systems). This includes the ability to program in at least one language and knowledge of basic computing systems. The four majors listed have these two items required as part of their degrees.

b. application and selection process;

Students from the four majors (CprE, Com S, SE, MIS) will be admitted to the minor by submitting a request. Students from other majors on campus can apply to the minor given they have the prerequisite course material. These applications will be reviewed by a small steering committee.

c. language requirements;

No additional language requirements

d. courses and seminars presently available for credit toward the program;

Com S 252: Linux OS Essentials
INFAS/Cpr E 332: Cyber Defense Competitions  
Cpr E 431: Introduction to Computer Security  
Com S 412: Formal Methods in Software Engineering  
CprE 308: Operating systems principles and practice  
Com S 352: Introduction to Operating Systems  

e. proposed new courses or modifications of existing courses;  
Add Cpr E 231: Cyber security concepts and tools  
Add Cpr E 430 Introduction to network security (Dual list of existing course CprE 530)  

f. advising of students;  
Students will be advised by the advisors in the Department of Electrical and Computer engineering;  

g. implications for related areas within the university.  
None

11. General description of the resources currently available and future resource needs, in terms of:

a. faculty members;  
The department has several faculty members that teach cyber security and the current faculty will teach the new courses.

b. computers, laboratories, and other facilities;  
The department will create a new laboratory to support the courses offered in the minor (CprE 231, 431, and 430). The department already supports the labs for 332, 431, and 530. However due to the increased enrollment the current lab environment is not sufficient to support the minor. The college and department will also provide computer support staffing to help run the new laboratory.

c. library facilities (journals, documents, etc.) in the proposed area;  
The library has numerous journals in the area of cyber security and no additional resources are needed.

d. supplies, field work, student recruitment, etc.  
The department and college already recruit students to focus on cyber security so no additional resources are required.

12. Describe the needs for new resources and/or reallocated resources. Attach to the program proposal memos from the department chair(s), the college dean(s), and other appropriate persons, agreeing to the allocation of new resources and/or the reallocation of resources.
The College of Engineering and the Department of Electrical and Computer Engineering have agreed to provide support for the creation of a new laboratory. In addition we are working with several companies to supply funding for equipment needed to create the Lab. In addition the college and department have agreed to provide the necessary IT support staff to maintain the lab. The Department of Electrical and Computer Engineering has agreed to provide the faculty support to teach the additional courses.

13. Attach to the program proposal, letters of support, recommendations, and statements when appropriate, from programs and departments at ISU which are associated with the proposed program or have an interest in the proposed program.

Department Chair ECpE
Department Chair Com S
Department Chair SCIS

14. If the new program is interdisciplinary, a governance document should be created and submitted to the Associate Provost for Academic Programs. Indicate here that it has been completed.

The proposed minor is not interdisciplinary as it is housed in and administered by the department of Electrical and Computer Engineering. The minor will have a steering committee consisting of faculty affiliated with the Information Assurance Center and the three departments whose students will be taking the minor. The steering committee will provide input as to the content of the courses and the new electives offered. This is the same steering committee that currently oversees the graduate security courses and degrees and current undergraduate courses to help ensure the courses and degrees are in alignment with current government security educational standards. (Our graduate degrees have been certified to meet the educational knowledge units specified by NSA/DHS.)
The Computer Curriculum Coordinating Committee has reviewed the proposal for the proposed minor in Cyber Security. As part of the review process input was obtained from the departments and colleges represented on the committee with includes Computer Science, Electrical and Computer Engineering, College of Liberal Arts and Sciences, College of Engineering, College of Business, College of Design. The committee members had no objections to the proposed minor.

Let me know if you have any questions.

--

Arne Hallam, Professor of Economics and Associate Dean College of Liberal Arts and Sciences
237 Catt Hall
Iowa State University
Ames, IA 50011

ahallam@iastate.edu

Work: 515-294-5861
FAX: 515-294-1303
Home: 515-292-8739
April 30, 2015

Faculty Senate Curriculum Committee
Iowa State University
Ames, IA 50011

To whom it may concern:

The Department of Electrical and Computer Engineering (ECpE) is enthusiastic in its support for proposed minor in Cyber Security. The faculty of the ECpE department met on March 6, 2015, and voted to support the minor. Of 54 eligible voting members, quorum was met, and the vote was unanimously positive (37 yes, 0 no, and 0 abstain).

The ECpE department will support the teaching of the courses required for the minor, and will provide support for the laboratory needed to teach the courses.

Sincerely,

David C. Jiles
Anson Marston Distinguished Professor
Palmer Endowed Department Chair
Department of Electrical and Computer Engineering
(515) 294-1097
dcjiles@iastate.edu
March 2, 2013

To: Whom it may Concern

Subject: Minor in Cyber Security

The Department of Computer Science is enthusiastic in its support for the proposed minor in Cyber Security to be offered by the Department of Electrical and Computer Engineering.

The Department of Computer Science has agreed to make two courses available to the minor and, if additional undergraduate security courses are created in its curriculum, it will work to include them as electives in the minor.

Sincerely,

Gianfranco Ciardo
Professor and Chair
Computer Science Department
Iowa State University
Ames, IA, 50011
(515) 294-3264
ciardo@iastate.edu
April 28, 2015

To Whom it may Concern:

The Supply Chain and Information Systems department is enthusiastic in its support for proposed minor in Cyber Security to be offered by the Department of Electrical & Computer Engineering.

Sincerely,

Sree Nilakanta
Chair
Academic Program Approval Voting Record

This document is to be appended as the last page of the proposal for any new or revised academic program to record the successive votes of approval as the proposal moves through its required review and approval steps. Consult Faculty Handbook Section 10.8 or the Faculty Senate Curriculum Committee website for information regarding Committee review and voting requirements for each action.

Curricular Action: (check appropriate boxes below)

1. X New Program  □ Name Change  □ Discontinuation  □ Concurrent Degree for:

2. □ Undergraduate Major  □ Graduate Major  X Undergraduate Minor  □ Graduate Minor
   □ Undergraduate Certificate  □ Graduate Certificate  □ Other: ___________________

3. Name of Proposed Change: ___Cyber Security_______

4. Name of Contact Person:  Doug Jacobson  e-mail address: dougj@iastate.edu

5. Primary College:  __Engineering___ Secondary College: ____________________

6. Involved Department(s):  __Electrical and Computer Engineering__

Voting record for this curricular action:

<table>
<thead>
<tr>
<th>Voting Body</th>
<th>Votes</th>
<th>Date of Vote</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For</td>
<td>Against</td>
</tr>
<tr>
<td>Dept. or Program Committee</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Dept. faculty</td>
<td>37</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>College Curriculum Committee</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>College Approval Vote</td>
<td>128</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graduate Council</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Faculty Senate Curriculum Committee</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>Faculty Senate Academic Affairs Council</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>Faculty Senate</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[FSCC – November 2013]