Period of reference in the template: 2006-07 to present

1. Please describe your program’s learning-outcomes trajectory since 2006-07: Has there been a transformation of organizational culture regarding the establishment of learning outcomes and the capacity to assess progress toward their achievement? If so, during which academic year would you say the transformation became noticeable? What lies ahead; what is the next likely step in developing a learning-outcomes organizational culture within the program?

[Please limit your response to 200 words or less]

This Minor program began as an initiative in the Center for Information Assurance and Security (CIAS), in coordination with the Computer Science (CSc) and Criminal Justice (CRJ) departments in the Spring 2006. The main purpose was for educating future criminal justice professionals in the area of computers and telecommunications, crime investigation, and evidence processing. The traditional CRJ program at CSUS has been successful in producing the work force for criminal justice. However, there has been a big trend of increased cyber crime, and consequently a great demand for the work force to investigate cyber terrorism, and cyber crime as well as industrial needs for such personnel.

The courses in the Minor are a combination of existing CSc courses along with three new proposed CSc courses. The intended audience includes, but not be limited to students in Criminal Justice, Management Information Systems, Business, Pre-Law, and Liberal Studies.

Original courses in this minor program in the program included: CSC 10, CSC 22, CSC 80, CSC 122, CSC 114, CSC 115, CSC 116. Recently the department reduced the number of courses to the following: CSC 1; CSC 8/8s or 80; CSC 15, 22, or 25; CSC 115; and CSC 116. Most of these courses have been assessed according to their clearly defined learning outcomes. The following are the expected learning outcomes of the minor program.

- Network and Internet security threats and countermeasures (CSC 115)
- Digital Evidence Management Methodology (CSC 116).
- Preparation of electronic evidence (CSC 116)
- Problem Solving (CSC 1, CSC 15/22/25, CSC 115, CSC 116)
- Team work (CSC 115, CSC 116)
- Life-long learning (CSC 1, CSC 15/22/25, CSC 115, CSC 116)
- Written and Oral communications (CSC 115, CSC 116)

2. Please list in prioritized order (or indicate no prioritization regarding) up to four desired learning outcomes (“takeaways” concerning such elements of curriculum as perspectives, specific content knowledge, skill sets, confidence levels) for students completing the program. For each
stated outcome, please provide the reason that it was designated as desired by the faculty associated with the program.

[Please limit your response per outcome to 300 words or less]

A) Network and Internet security threats and countermeasures - Knowledge of computer network security threats and how to defend against them is at the core of the Information security and computer forensics minor program.

B) Problem solving – The ultimate goal of this program is to enable students to acquire the ability to develop practical skills in solving real-world cyber security problems especially with respect to dealing with response to cyber security incidents (eg. Attacks, intrusions, etc.)

C) Digital Evidence Management Methodology – Students need to understand the standard methodology, techniques, and tools for management the digital evidence life cycle.

D) Life-long learning – Cyber security is tied to fast advances in new technologies since new technologies bring with them new security threats. This program gives students first-hand experience to understand that life-long learning is critical for an educated person in general, and a cyber security professional in particular.

3. For undergraduate programs only, in what ways are the set of desired learning outcomes described above aligned with the University’s Baccalaureate Learning Goals? Please be as specific as possible.

[Please limit your response to 400 words or less]

The relationship between our four desired learning outcomes and the University’s Baccalaureate Learning Goals (BALG) is represented in the matrix below linking desired learning outcomes with BALG. Each BALG is linked with one or more learning outcomes.

<table>
<thead>
<tr>
<th>University Baccalaureate Learning Goals</th>
<th>Outcome (a) Network and Internet security threats and countermeasures</th>
<th>Outcome (b) Problem solving</th>
<th>Outcome (c) Digital Evidence Management Methodology</th>
<th>Outcome (d) Life-long learning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competence in Discipline</td>
<td>X</td>
<td>X</td>
<td>x</td>
<td>X</td>
</tr>
<tr>
<td>Knowledge of Human Cultures &amp; Physical &amp; Natural Worlds</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Intellectual &amp; Practical Skills</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Personal &amp; Social Responsibilities</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Integrative Learning</td>
<td>X</td>
<td></td>
<td>x</td>
<td>X</td>
</tr>
</tbody>
</table>
Competence in the Discipline:

Outcome A involves the ability to apply knowledge of computer science (a related field) to fundamental areas in information security, such as, information security threats, defense of information systems to reduce risks, and dealing with security incidents. This ability is demonstrated in understanding the tradeoffs required in the effective solutions to information security problems.

Outcome B involves skills required to apply the fundamental knowledge in outcome (a) in the analysis, design, and development of computer-based systems that satisfies requirements.

Knowledge of Human Cultures and Physical and Natural Worlds:

Outcome A requires graduates of the minor program to have knowledge of computer systems and how it interacts in the real world. For instance ways of handling security incidents usually begins with formulation of policies and ethical behavior. In addition, is assumed that all graduates of this program complete the standard CSUS General Education requirements.

Intellectual and Practical Skills:

This BALG is addressed by all four desired outcomes. Outcomes A and B cover the intellectual and practical skills of inquiry and analysis, critical thinking, and problem solving. Outcome C involves teamwork and Outcome D effective oral and written communication skills.

Personal and Social Responsibilities:

Outcome B is related to analytic abilities in problem solving which address ethical reasoning and real world challenges. Outcome C teamwork addresses “the ability to work collaboratively with those from diverse cultural backgrounds”, a common work environment in technical disciplines such as information security.

Integrative Learning:

Interdisciplinary learning are evident in most of the Outcomes which addresses a student’s ability to integrate knowledge and skills acquired in information security and to apply such skills in the development of a system. The ability to effectively communicate this knowledge, Outcome D, is a critical part of integrative learning.

4. For each desired outcome indicated in item 2 above, please:
   a) Describe the method(s) by which its ongoing pursuit is monitored and measured.
   b) Include a description of the sample of students (e.g., random sample of transfer students declaring the major; graduating seniors) from whom data were/will be collected and the frequency and schedule with which the data in question were/will be collected.
c) Describe and append a sample (or samples) of the “instrument” (e.g., survey or test), “artifact” (e.g., writing sample and evaluative protocol, performance review sheet), or other device used to assess the status of the learning outcomes desired by the program.
d) Explain how the program faculty analyzed and evaluated (will analyze and evaluate) the data to reach conclusions about each desired student learning outcome.

[Please limit your response to 200 words or less per learning outcome]

(If the requested data and/or analysis are not yet available for any of the learning outcomes, please explain why and describe the plan by which these will occur. Please limit your response to 500 words or less.)

We have not yet performed assessment for this program. We plan to do so in the 2012-2013 academic year. The department has done significant and extensive assessment for the undergraduate and graduate programs. We can make use of the department expertise to perform assessment of this minor program.

5. Regarding each outcome and method discussed in items 2 and 4 above, please provide examples of how findings from the learning outcomes process have been utilized to address decisions to revise or maintain elements of the curriculum (including decisions to alter the program’s desired outcomes). If such decision-making has not yet occurred, please describe the plan by which it will occur.

[Please limit your response to 200 words or less per item]
a)
b)
c)
d)

Given that there is no data as specified in section 4 we do not have adequate information to report here. We plan to do so in the future.

6. Has the program systematically sought data from alumni to measure the longer-term effects of accomplishment of the program’s learning outcomes? If so, please describe the approach to this information-gathering and the ways in which the information will be applied to the program’s curriculum. If such activity has not yet occurred, please describe the plan by which it will occur.

[Please limit your response to 300 words or less]

This important program is relatively young in our department. We anticipate attracting an increasing number of students. We are working on an outreach plan for the campus at large.

The department has an active Industrial Advisory Committee (IAC). We plan to work with IAC on this task as well.
7. Does the program pursue learning outcomes identified by an accrediting or other professional discipline-related organization as important? Does the set of outcomes pursued by your program exceed those identified as important by your accrediting or other professional discipline-related organization?

[Please limit your response to 300 words or less]

N/A

8. Finally, what additional information would you like to share with the Senate Committee on Instructional Program Priorities regarding the program’s desired learning outcomes and assessment of their accomplishment?

[Please limit your response to 200 words or less]

As mentioned in section 1 this Information Security and Computer Forensics Minor program began as an initiative within the Center for Information Assurance and Security (CIAS), in coordination with the Computer Science (CSc) and Criminal Justice (CRJ) departments in the Spring 2006. CIAS has been designated jointly by the US Department of Homeland Security and National Security Agency as a national Center of Academic Excellence (CAE) in Information Assurance and Security Education since 2007. The designation is for 5 years and we just renewed our application. In order to receive the designation the department had to map its information security course offerings to national standards as well as satisfy 10 benchmarks including interdisciplinary nature of our program. This means that information security knowledge units reach outside the boundaries of our department and the college. This makes the minor program imperative. Specifically, the main purpose of this minor program is for educating future professional such as those in criminal justice and business in the area of computers and telecommunications, crime investigation, and evidence processing.

This minor program in information security and computer forensics has the potential to help to spread cyber security knowledge to as many students on the entire campus as possible. This will in turn bolster our efforts to maintain the status of our Center of Information Assurance and Security (CIAS) as a Center of Academic Excellence (CAE) by the Department of Homeland Security and the Nation Security Agency. Our CAE designation has brought a number of grants and consulting opportunities to the department including $1.2 million dollars from NSF for scholarships for 15 students over 3 years, grants for cyber security research for smart grid, forensics investigation of computers for a number of California state agencies, training information security officers for a number of state agencies to name a few major ones. As indicated in prior sections we are working on marketing this minor program to a wider audience on campus. Finally, we wish to state that the two major courses in the minor (CSC 115 and CSC 116) can be used to satisfy electives in the Criminal Justice Division. We are planning to work with other departments such as business along similar lines.