PROGRAM NAME: **Information Systems CyberSecurity** ACADEMIC YEAR: **2013 - 2014**

INSTRUCTIONAL PROGRAM REVIEW

The timeframe of program review is five years, including the year of the review. Data being reviewed for any item should go back the previous four years, unless not available. Questions regarding forms, calendars & due dates should be addressed to the I.E. Department.

I. PROGRAM RELATIONSHIP TO THE COLLEGE MISSION & STRATEGIC PLAN

A. Describe how the program supports the college mission and core values.

A$_1$. Supporting the Collin College Mission

Collin County Community College District is a student centered and community centered institution committed to developing skills, strengthening character, and challenging the intellect.

Collin College's cybersecurity programs are designed to produce successful students with fundamental knowledge of computer network security function and design. Throughout the program, students are intellectually challenged to learn the conceptual and practical knowledge required to serve the information technology security needs of businesses within the college's service area. Important components of these programs are the development of skill sets and behaviors that develop the student's professional character that local businesses are expecting to find.

A$_2$. Supporting Collin College Core Values

The Information Systems Cybersecurity programs support Collin's core values in various ways. The programs offer a wide breadth of opportunities to learn using a number of techniques. In addition to the customary face-to-face classroom environment, delivery can be done via Web-based online classes, involving self-study with faculty mentoring. Hybrid classes which join the traditional face-to-face classroom environment with modern online instruction are also available.

The Information Systems Cybersecurity faculty provides community service and involvement by offering to juniors and seniors in local high schools an opportunity to take cybersecurity courses common to both the Information Systems Cybersecurity program at Collin College and the career and technical education departments within the local school districts. This allows high school students the opportunity to get an early start on their educational goals. Faculty members also lend their support to community service through their involvement in student organizations like the National Technical Honor Society as well as the Information Systems Security Association (ISSA), a professional Security organization.

The Information Systems Cybersecurity program faculty members adhere to high standards of learning by routinely educating themselves about contemporary trends and technological advancements within the field of cybersecurity. Given the highly dynamic nature of the threats faced by modern information technology infrastructure, this is a constant requirement for the cybersecurity professional. The program adheres to the core value of creativity and innovation by continuously creating new content, enhancing existing courses, and introducing innovation into course delivery. As an example, faculty members capitalize upon on computer virtualization technologies along with the Blackboard learning management system to expand options for students in the program's Security+ course.

The Information Systems Cybersecurity faculty members believe their high standards for integrity are a key factor in the dramatic increase in the program's student enrollment. Integrity and professional character are key components in the curriculum for the Information Systems Cybersecurity program. Students learning how to prevent network intrusion attacks become quite familiar with the techniques used by malevolent actors in this environment, and it is routinely emphasized for students that their knowledge of these techniques should not be used in a malicious fashion simply because the students are knowledgeable of them.

The cybersecurity program maintains demanding and strict academic standards for our students in order to maintain academic excellence within the program. This effort has flowed into the community as evidenced by local companies offering our students internship, permanent hire, promotion, and internal transfer positions based upon the knowledge they have gained from their Information Systems Cybersecurity courses.

Cybersecurity program faculty treat all students with dignity and respect regardless of their current position in life: current high school students, recent high school graduates, career transition students, or returning veterans, et al. While Collin's goal is to provide its students with a top notch technical education to provide them a formidable start in a new career, the success of each student requires that the faculty emphasize the importance of individual integrity and accountability while providing an environment that encourages learning-from-failure in order to afford the student's future employer the best opportunity to achieve its mission critical goals. Finding this balance requires that faculty members demonstrate dignity and respect in the classroom on a daily basis.

B. Describe how the program supports the college strategic plan.

The Information Systems CyberSecurity program directly supports Collin College's strategic plan in a number of ways. Strategic goal #1 for the 2016 Strategic Plan is to improve academic success by implementing strategies for completion. The Information Systems Cybersecurity program has instituted three levels of credentials that a student can choose to pursue in order to meet their career objectives. The AAS degree is a two-year degree (comprising 71-72 semester credit hours) that prepares students for a career in cybersecurity. Upon completion of the program a graduate will be able to a.) design and install se cure network systems based upon customer requirements, b.) monitor and maintain network traffic and security, and c.) maintain network hardware and software. In addition to these specific technical skills, the program requires students to complete a general education component of 16 semester credit hours to develop a variety of general education competencies including writing, mathematical reasoning, and speech communication skills, among others. For those students desiring to learn the fundamentals of cybersecurity without pursuing a formal two-year degree, the program offers the Certificate in Information Systems Cybersecurity. This program requires 39-40 semester credit hours for completion, can be used to round out a student's prior formal education or career knowledge by focusing each student's efforts on learning the fundamental tenets of cybersecurity without requiring the general education courses that are present in the AAS degree. Finally, for those students that may already have made a career change into cybersecurity, the program offers the CISSP Information Systems Cybersecurity Professional Certificate. This program comprising a total of 15 semester credit hours prepares students to sit for three crucial industry certifications (Network+, Security+, and Certified Information Systems Security Professional (CISSP)). This collection of industry recognized certifications will allow students to obtain professional level recognition of their expertise in a short amount of time. By providing multiple levels of completion milestones, students can choose to pursue the program best suited to their current career needs and the most efficient use of their time.

Collin's Strategic Goal #2 is to provide access to innovative higher education programs that prepare students for constantly changing academic, societal, and career/workforce opportunities. The Information Systems Cybersecurity program pursues this goal by routinely updating the content of program coursework. Recently, program faculty have introduced semester projects for ITSY 2300-Information Systems Security and ITSY 2341-Security Management Practices. These projects present the student with a problem of current interest in the field of cybersecurity. The students are tasked with providing a solution to the problem that draws upon the lessons learned in that specific course as well as required prerequisite courses. In addition, faculty members have recently made considerable improvements in the technology covered in ITSY 2301-Firewalls and Network Security with the donation of next-generation firewalls from Palo Alto Networks. The improvement in the level of instruction that this equipment has provided prompted the faculty to pursue being named Palo Alto Networks Academy. The development of these types of curricular enhancements ensure that students completing the program are encountering the most modern cybersecurity technologies to ensure relevance with industry needs.

Collin's Strategic Goal #3 is to engage faculty, students, and staff in improving a districtwide culture of adherence to the Collin College Core values. As noted earlier program faculty members maintain considerable efforts to remain current on the state of cybersecurity industry trends and technologies, participating in service and involvement within the college community and within the wider professional cybersecurity community, exhibit creativity and innovation within their course designs and course delivery methods, encourage academic excellence among program students, treat all students, faculty and staff members with dignity and respect, and maintain an environment of consistently high integrity. With respect to this latter core value, the Information Systems Cybersecurity program is somewhat unique in that students are routinely investigating how to track down incidents of unapproved penetration of computer network infrastructure. A byproduct of this knowledge is that program students are routinely learning about techniques and methods used to carry out these attacks. Program faculty members routinely remind students of the ethical obligation not to utilize this knowledge in a malevolent manner.

Finally, Collin's Strategic Goal #4 is to enhance the College's presence in the community by increasing awareness, cultivating relationships, building partnerships and developing resources to respond to current and future needs. The Information Systems Cybersecurity program has routinely gone to considerable lengths to reach out to the community via a wide array of initiatives. First, this program has been instrumental in reaching out to area school districts to offer technical dual credit courses on site at the high schools to provide students an opportunity to learn more about cybersecurity and the career opportunities that exist in this rapidly growing field. In addition the program has taught courses onsite at two businesses in the region to make required training available in a timely and convenient format. The cybersecurity program has reached out to various professional organizations, including the

Information Systems Security Association (ISSA) to inform local professionals of the program's course offerings, and this effort has recently resulted in the development of a student chapter of the ISSA at Collin College. This student chapter is only the second student chapter of its kind in the United States. Finally, program faculty members have utilized the relationships in the region to develop a series of regular invited lectures by Information Systems Security professionals on topics of current interest. This has helped to bring these professionals on campus and it has given them an opportunity to better understand the capabilities of Collin's cybersecurity program students.

II. PROGRAM CURRICULUM

Sections A, B & C apply only to workforce programs.

A. Attach all course syllabi with SCANS included. (Workforce Programs only)
Exhibit: **II Combined CyberSecurity Program Syllabi**

B. Show evidence that the THECB standards listed below have been met. For any standard not met, describe the plan for bringing the program into compliance. (Workforce Programs only)

1. Credit Hour Standard: There are no more than 60 credit hours in the program plan.

Number of semester credit hours (SCH) in the program plan: 71 – 72 # of SCH .

If there are more than 60 SCH in the plan, show revision of curriculum. Work with the program's curriculum coordinator to bring the revised program plan to the Curriculum Advisory Board (CAB).

At the time of this review, the CyberSecurity program, a 71-72 credit hour program, is being appraised and in process for CAB approval. Is undergoing discussions with faculty and the industry advisory board to get the program to 60 SCH.

2. Completers Standard: Average 25 completers over the last five years or five completers per year.

Number of completers: 21 AAS/Certificate completers in the last five years

If below the state standard, attach a plan for raising the number of completers by addressing barriers to completion and/or by increasing the number of student enrolled in the program. Definition of completer—Student has met the requirements for a degree or certificate (Level I or II)

a. The Information Systems Cybersecurity program is a recent addition at Collin College. We had no completers during fiscal year 2009 or 2010. In fiscal year 2011, there were 7 AAS/Certificate completers, in 2012 there were 7 AAS/Certificate completers, and in 2013 there were 7 AAS/Certificate completers. Thus, over the last three years, we have been above the state mandated standard of five completers per year. We have seen enrollment increase in the program courses over the last two years. The program will be adding a new FT instructor in Cybersecurity to increase the availability of program courses. Over the last five years, there have also been a total of 12 completion certificates for the AAS core by students that have declared Information Systems Cybersecurity as their intended major.

3. Licensure Standard: 90 % of first time test takers pass the Licensure exam.

If applicable, include the licensure pass rate: Enter % -- **NOT APPLICABLE** (we have certifications not licensures)

For any pass rate below state standard, attach a plan for raising the pass rate.
Enter plan to raise the pass rate here.

C. Current Curriculum (Workforce Programs only)

1. Is the program curriculum up-to-date? Please review Collin College's program curriculum at the following levels:

a. Compared to similar programs at peer schools,

The only local Community College that offers any type of security program is Richland College in the Dallas Community College District. Richland College offers two degrees and two certifications. An assessment of the degrees offered by each college reveals a completely different philosophical approach. Collin College focuses on prevention of network attacks centered on both hardware and software; whereas, Richland College offers studies on analyzing forensic data to analyze why prevention fails. It appears that the degree at Collin College and the degree at Richland College only complement one other. Therefore, a course by course comparison and a degree by degree comparison do not provide equivalency between our programs.

b. Compared to the first two years of baccalaureate requirements in related fields at Collin College's top ten transfer institutions or existing articulation agreements, and

The top ten transfer institutions for Collin students in 2011-2012 can be found at**:**

http://www.collin.edu/aboutus/statistics/TopTransferInstitutions.html

In decreasing order of importance (in terms of number of transfers):

1. UT-Dallas
2. UNT
3. Texas Women's University
4. Texas A&M-Commerce
5. UT-Arlington
6. Texas A&M
7. UT-Austin
8. Univ. of Arkansas
9. Texas Tech Univ.
10. Texas State Univ.

The only member of this group that will accept coursework from the CyberSecurity program at Collin is the BAIT program at UNT. The courses that will be accepted 21 SCH of WECM courses in addition to Gen Ed core courses.

In cybersecurity, we do have signed articulation agreements with Western Governor's University and via the DOL Grant **Exhibit: Touro University Worldwide.** (**Exhibit: IICb3 TUW Collin College MOU_1**) These are both accredited online institutions that will accept on the order of 60 SCH from Collin's CyberSecuirity program toward Bachelors degrees.

(Exhibit: IICb3 WGU-Collin College Guaranteed Pathway College)

c. Any professional association standards or guidelines that may exist relevant to the program.

If the program curriculum differs significantly from these benchmarks, explain how the Collin College curriculum benefits students and other college constituents.

In Information Systems Cybersecurity, we adhere to the International Information Systems Security Certification Consortium (ISC)^2 Code of Ethics

Code of Ethics Preamble:

- The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

2. Advisory Committee

a. How many employers does your Advisory Committee have? Enter # of employers 10

CyberSecurity Advisory Board

Mike Saylor		Cyber Defense Center
Patrice Alessandra		Dell Systems
Russ Murrell	Co-Chair	Dell Systems
Steve Levesque		Dell Systems
Kevin Mellott		Erase.com
Ronald Kopeki		Global Data Guard
Mack Williamson		HP
Joe Estensen		Oncor Electric
Jason Rowe		Palo Alto Networks
Mike Ancelin		Palo Alto Networks
Bryan Humphreys		Path Way Enterprises
Mark Johnson		Raytheon
Randy Herbert		Raytheon
Steve Austin		Raytheon
Wayne Boline		Raytheon
William Jackson		Raytheon

John Jordan	Co-Chair	TI

How many attended the last two meetings? 10 Enter # that attended the last two meetings.

Have they contributed any resources to the program (time, equipment, supplies, money, co-op spots)?
☒ Yes □ No If Yes, briefly describe contributions in Table V.

b. Status of Advisory Committee curriculum recommendations:

Briefly summarize the curriculum recommendations made by the Advisory Committee over the last five years.

As this program was just being built 4 to 5 years ago, the CyberSecurity Advisory Board has been instrumental in terms of relevant curriculum recommendations from each respective member's corporation' s perspective. The high lights of the recommendations are below. The status of implementation is noted.

- Recommended to include a Security + Certification course- **Implemented**
- Recommended to include ITIL Certification- **Not Implemented**
- Recommended to include a CISSP Certification elective course- **Implemented**
- Recommended to build a CISSP Professional Certificate- **Implemented**
- Recommended to include an on-line Security + Certification course- **Implemented**
- Recommended to include a Cloud Essentials Certification course- **Implemented**
- Recommended to include a VMWare Certification course- **Implemented**
- Recommended to include a CISM Certification course**- In Process of Implementation**
- Recommended to change from Microsoft Server 2003 course work to Microsoft Sever 2008 coursework- **Implemented**
- Recommended to change from Microsoft Server 2008 course work to Microsoft Sever 2012 coursework- **Scheduled for Fall 2015 Implementation**
- Recommended to include a CyberSecurity Case Study course- **Not Implemented**
- Recommended to include Palo Alto Networks curriculum into Firewalls course- **Implemented**
- Recommended to become a Palo Alto Networks Academic Academy- **Implemented**

- Recommended to bring CyberSecurity track to local ISD's High School Career Pathways- **Implemented Fall 2013, Fall 2014 or Fall 2015 depending on the ISD.**
- (Based on State of Texas requirement to take AAS degrees to 60 hours) Recommended to make all 4 credit courses 3 credits- **Implemented**
- Recommended that students need a "Private Cloud Ecosystem" in which they can work with security threats (viruses, malware, Trojans, etc.). In a segmented environment, the student could learn without fear of harm to the external environment.- **Not Implemented**

Exhibit: IIC2b1 CyberSecurity Advisory Committee Minutes Friday December 16_2011
Exhibit: IIC2b2 CyberSecurity Advisory Committee Minutes Friday February 10_2012
Exhibit: IIC2b3 CyberSecurity Advisory Committee Minutes Friday June 8_2012
Exhibit: IIC2b4 CyberSecurity Advisory Committee Minutes Wednesday December 14_2012
Exhibit: IIC2b5 CyberSecurity Advisory Committee Minutes Wednesday August 14_2013
Exhibit: IIC2b6 CyberSecurity Advisory Committee Minutes Wednesday December 11_2013

Briefly explain why any Advisory Committee recommendations were not followed (budget limitations, prohibited by accrediting bodies or regulations, not feasible, not appropriate for college mission, lack of qualified faculty, etc.).

- Recommended to include ITIL Certification- **Not Implemented- Study showed too few students in DFW Metroplex to justify effort.**
- Recommended to include a CyberSecurity Case Study course- **Not Implemented- Advanced Computer Networking Case Study capstone class was modified to include CyberSecurity**
- Recommended to include a CISM Certification course**- In Process of Implementation- Professor had to be credentialed before teaching the class. Student poll has not indicated that enough students want this certification to make a class at 15.**
- Recommended to change from Microsoft Server 2008 course work to Microsoft Sever 2012 coursework- **Scheduled for Fall 2015 Implementation- On track.**
- Recommended that students need a "Private Cloud Ecosystem" in which they can work with security threats (viruses, malware, Trojans, etc.). In a segmented environment, the student could learn without fear of harm to the external environment.- **Not Implemented- Halted based on high dollar cost. At present, we are looking for funding sources.**

How might these barriers to implementation be overcome, if appropriate?

The below recommendation is the only recommendation where a barrier has stopped implementation. We are actively seeking the funds to pursue this pathway.

- Recommended that students need a "Private Cloud Ecosystem" in which they can work with security threats (viruses, malware, Trojans, etc.). In a segmented environment, the student could learn without fear of harm to the external environment.- **Not Implemented- Halted based on high dollar cost. At present, we are looking for funding sources.**

3. Provide the program-level SCANS matrix or a curriculum map that shows every program outcome is supported by at least two courses and every course supports at least one program outcome to demonstrate that the program curriculum sufficiently addresses the acquisition of the foundational skills and knowledge required for students to achieve competency in the program outcomes?
Exhibit: **IIC3 Information Systems CyberSecurity AAS_SCANS Crosswalk_1_1**

D. What are the completion barriers in the program curriculum? (All instructional programs)
Go to the Program Review page on CougarWeb and select the program course history for each of the program awards. Links to the Program Review page are found on both the Institutional Effectiveness and Teaching & Learning pages.

1. Review the course retention rate, course success rate, course enrollment and periodic scheduling to identify barriers to program completion.

a. Program course retention rate: Attach print out and identify any courses that have a retention rate below the state standard.

Exhibit: **IID1a Cybersecurity Retention, Completion, Success**

All course retention rates in technical courses are greater than 70%.

b. Is there sufficient course enrollment to support a stable cycle of required course offerings?

☒ Yes ☐ No

Show course enrollment for technical or field of study courses.

Exhibit: **IID1a Cybersecurity Retention, Completion, Success**

Over the last three academic years course enrollment for technical classes are consistently getting above 15. The only exception is ITSY-2343 in Spring 2013 with an enrollment of 14. This is expected to continue growing as the program expands in Spring 2014 will run 2 sections with 37 students enrolled.

For any required program courses with enrollment below 15, explain a plan to grow enrollment or revise the curriculum.
N/A - there are no programs with less than fifteen student.

c. Are the required courses in the program offered at intervals appropriate to enable students to complete "on time" if a student was enrolled full-time and followed the degree plan? ☒ Yes □ No

d. Identify any required program courses which frequently require course substitutions to enable students to complete an award. None

2. Considering the course retention information gathered from step 1 above, explain program changes planned to remove or mitigate any observed barriers. NO Barriers – given retention, completion, and success rates, there are no obvious barriers in the program.

.

III. PROGRAM INFORMATION: ARE THE PROGRAM LITERATURE AND ELECTRONIC SITES CURRENT AND DO THEY PROVIDE AN ACCURATE REPRESENTATION?

A. Provide program website **url: http://www.collin.edu/academics/programs/cybersecurity.html**

B. List all program literature (course descriptions, degree plans, catalog entries, etc.) in the table III below.

C. Provide the review date (within the last three months) in Table III below that shows the elements of information listed on the website and in brochures were checked and updated for accuracy (current academic calendars, grading policies, course syllabi, program handouts, program tuition costs and additional fees, description of articulation agreements, availability of courses and awards, and local job demand in related fields) are accurate and available to the public.

Table III-Program Literature Review – **See Exhibit: III Program Literature View Program Literature View**

IV. EMPLOYMENT FOR PROGRAM GRADUATES

A. Provide evidence of local demand for program graduates.

Enter evidence here. (from: Career Coach – fifty mile radius from Frisco, TX)

Job Title	Estimated Local Annual Openings within 50 miles	Median Salary / per hour
Computer Security Manager	308	59.70
Computer Systems Security Analyst	124	38.83
Homeland Security Program Specialist	8	33.03
Information Systems Cybersecurity	723	38.05
Network Security Administrator	494	37.09
Network Security Analyst	151	43.04
Security Architect	182	41.92
Security Management Specialist	1,036	34.80
Security Specialist	268	32.82

If there is low current demand, as evidenced by few AAS-level job postings, explain why and show evidence that near-term future demand will improve local demand for graduates of this program.

There appears to be robust demand for program graduates. No action necessary.

B. What percent of graduates secure employment in the field? 30-45% employed in 2011 and 2012 per Measure 3

If the employment rate is below 75% within 12 months of graduation, explain the plan to increase employment of the program's graduates through relationship building.

Given the relatively small numbers of graduates that the program is currently producing each year, the reported employment rate is highly dependent upon identifying every single graduate. (For example, in FY 2012, seven AAS degrees or certificates were awarded. Failure to find two of these students in the Texas

Workforce Commission databases will result in an employment rate of less than 75%.) Over the last two-three years, the program has seen continually rising enrollments in the courses that comprise the program, and we are seeing steadily increasing numbers of students progressing through the program each year, so this problem should begin to abate in the near future. Another point to keep in mind is that the TWC databases only identify students that are employed within the state of Texas. If a graduate is employed but immediately transferred out of state the reported employment number can be negatively influenced. While an increasing number of completers should help to alleviate this problem in the near future, this issue could persist depending upon the sizes of the employers of our graduates. (If a large number of national or multinational businesses hire our graduates, we could find significant numbers of graduates not turning up within the TWC databases.

C. Average salary of program graduates. **Unknown** Avg Salary

If average salary is at or below minimum wage plus 15%, explain how the program will be modified to add economic value for graduates.

The Gainful Employment Placement Rate statistics reported by the Texas Higher Education Coordinating Board identified all four of the Cybersecurity certificate holders that received their award during fiscal year 2011. During the fourth quarter of calendar year 2011, these four certificate holders were compensated with a mean annual wage of $59,575. While this is clearly well above the minimum threshold indicated above, the very small sample size is difficult to extrapolate to all of the AAS/certificate completers. The certificate holders represent only 19% of all AAS degree/certificate completers for the five-year reporting period. We have no data reported for any AAS degree completer, and the certificate holders may represent graduates that already possess considerable experience within the Information Systems field. This fact alone demonstrates that the THECB-reported number may be skewed and may not be representative of the entire cross-section of program completers.

D. Average number of months to employment. **Unknown** # months to employment

If the average time to employment exceeds six months after graduation, describe the plan to support employment searches for upcoming (and recent) graduates.

This data is not currently available for program graduates.

E. What actions do the program personnel take to assist the college in obtaining the information required by Title IV and Gainful Employment so that students enrolled in this program are able, if otherwise eligible, to receive federal financial aid? Program faculty members report to Collin's Institutional Research Office the names of any recent graduates and their employers if the student has self-identified this information to the faculty members.

F. What additional actions, if any, are needed to improve the quality of this programs' information needed for college federal reporting requirements?

Enter additional actions here.

It does not appear that the program can assist in any greater degree w/o additional guidance from IRO,

Program Data:

Unduplicated, actual, annual enrollment data;

Definitions of data elements can be found on CougarWeb under Teaching & Learning/Program Review/Institutional Research Files for Program Review.

- Student/Faculty Ratios:
  From fiscal year 2009 to fiscal year 2013 the student-faculty ratio has increased from 2.0 (fall 2008) to 4.1 (fall 2013), reflecting increasing student enrollments in program courses over the time frame measured. These numbers are quite low in absolute magnitude because of the measure being defined as the number of FT equivalent students to the number of FT equivalent faculty members. (It should also be noted that ITSC 1305 and ITSC 1309 should not be included in any of the enrollment numbers for Information Systems cybersecurity, as those courses are not and never have been included in the program.)

  Exhibit: IVpd1 Measure 4 Student faculty ratio

- Average Class Size by course:
  From fiscal years 2009-2013 course enrollments for the computer networking courses have generally grown from 6.0-22.7 students in Fall 2008 to 13.8-24.0 in Spring 2013. Average enrollments in the most popular courses (ITCC courses) appear to be abnormally low due to the fact that Continuing Education has a minimum of 5 seats in every ITCC course, and in some semesters certain sections may have considerably more. (A common range of CE students in ITCC courses ranges from 3-12 for a given section in any one semester.) Since the enrollment numbers we are reporting only account for credit students, the average section enrollment that is reported is lower than the number of students that we are serving. Enrollments for the ITSY courses (cybersecurity-specific courses) have also expanded dramatically. During the entire 2009 fiscal year, only one ITSY course (ITSY 2300) was offered with an average enrollment of 12.0 students. During fiscal year 2010, six ITSY courses were offered with average enrollments of anywhere from 9.0 to 20.0 students, and by Fiscal year 2013, seven ITSY courses were offered with average enrollments of 14.0 to 42.0 students. This enrollment growth reflects a genuine attention to the development of this program as an extension of the Engineering Technology department’s fundamental expertise in computer networking and the expansion of interest in cybersecurity careers in the last two or three years..

  Exhibit: IVpd2a Measure 5 Average Class Size by Course

- Average class size for programs:

Over the period from fiscal year 2009 - fiscal year 2013 the average class sizes for all program courses has grown from 13.6 to 17.4, with an average class size over all fiscal years of 16.2. This number reflects the issue associated with ITCC courses and continuing education students noted above, so the real number is somewhat higher than the reported value. Most importantly, the trends observed in the exhibit reflect once again the overall growth in student demand for this program.

Exhibit: IVpd2b Measure 5 Average Class Size for Programs by Term.

- Course Enrollment History for all program courses (workforce programs may exclude reporting core course enrollments):
Overall duplicated enrollments in Information Systems Cybersecurity courses have increased dramatically during the period from fiscal year 2009 to fiscal year 2013. Since computer networking courses contain students that intend to pursue majors in our computer networking programs, we will restrict our discussion to the ITSY courses in this section. Consistent offerings of seven of the ITSY courses required for the AAs degree have occurred in the last two years, and the expanded offerings can be seen in Measure 1a where enrollments in all ITSY courses have grown during the last five years. (ITSY 1400 enrollments grew from 0 to 139, ITSY 2300 enrollments grew from 31 to 54, ITSY 2301 enrollments grew from 0 to 19, ITSY 2341 enrollments grew from 0 to 25, ITSY 2342 enrollments grew from 0 to 22, ITSY 2343 enrollments grew from 0 to 14, and ITSY 2371 enrollments grew from 0 to 17) ITSY 2572 has been a little more sporadic with enrollments of 0, 33, 30, 29, and 0 in the last five fiscal years. This reflects the specialized nature of this course and the fact that it was being offered in a 16 week format, unlike the situation for the other ITSY courses that are offered in 8 week terms. We believe that this may have caused scheduling conflicts for some students, and so we have switched over to offering this course in an 8 week format in Spring 2014. The course ran successfully with 18 students under this approach.

Exhibit: IVpd3a Measure 1a Program Enrollment Duplicated Enrollment
Exhibit: IVpd3b Measure 1b Program Enrollment Unduplicated Enrollment

- Grade Distributions:
Grade Distributions for the Information Systems Cybersecurity courses reflect a consistent application of faculty grading policies. Overall, the grade distributions during long semesters, for all courses within the program reflect that approximately 40% of students earn grades of “A”, 20-30% of students earn grades of “B”, 5-10% of students earn grades of “C”, 0-2.5% of students earn grades of “D”, and 10-20% of students earn grades of “F”. Typically 4-10% of students undertake withdrawals in any given long semester. The consistency of these distributions is also reflected in the fact that generally 90-95% of students complete their courses and anywhere from 70-80% of students earn grades of “C” or better for courses taken during the long semesters. This overall distribution is consistent with other workforce programs at Collin College. The grades that students earn in ITSY courses are somewhat higher than the grades earned in the foundational computer networking courses. We believe that this reflects the fact that these networking courses are typically taken during the 1st half of the AAS program and the ITSY courses are typically taken during the latter half of the AAS program. Since the students have generally been required to successfully complete the networking courses, they have learned invaluable study skills and better understand faculty expectations when moving into the cybersecurity-focused portion of the curriculum.

Exhibit: IVpd4 Measure 6a-6b Grade Distribution Completion & Course Success Rate by Term

- Contact Hours Taught by Full-Time and Part-Time Faculty:
  Full time faculty have traditionally taught 60-75% of all contact hours in computer networking (including ITSY courses). As of Fall 2013, the ratio was 66% full-time and 33% part time. Given the general growth in student demand for the Information Systems Cybersecurity program, we will be adding an additional full-time faculty member in cybersecurity for fall 2014. Generally the college tries to maintain a rough 50:50 ratio in contact hours taught by FT and PT faculty members, but the highly specialized nature of many computer networking professionals, and the particularly specialized nature of cybersecurity professionals makes this a difficult ratio to obtain, due to a limited number of professionals willing/able to serve on our associate faculty.

Exhibit: IVpd5 Contact Hours – Measure 7 Contact Hours Taught by FT-PT Faculty Fall 2009

V. PROGRAM RESOURCES SINCE LAST PROGRAM REVIEW

A. Partnerships and Relationship Building: List all university/business and industry partnerships. Include co-op or internship sites, visiting class presenters, tours of facilities' use, equipment donors, dedicated program scholarship donors, mentors.

Table V-A: Partnership Resources

University/Business & Industry	Partnership Type	Estimated Market Value, if any
Alcatel-Lucent- Security Operations Center	Co-op (3 students placed)	N/A
Palo Alto Networks	12 Firewall Devices	~$ 32 K
Palo Alto Networks	Academic Academy Designation	N/A
Kevin Mellot, Erase.com	Speaker At Engineering Speaker Series	N/A
Matt Hester, Microsoft Corp.	Speaker At Engineering Speaker Series	N/A
Leo Lorenz, Cisco Corp.	Speaker At Engineering Speaker Series	N/A
Ed Reynolds, HP Enterprise Solutions	Speaker At Engineering Speaker Series	N/A
Nick Piagentini. Palo Alto Networks	Speaker At Engineering Speaker Series	N/A

Rick Brunner, GM Financial	Speaker At Engineering Speaker Series	N/A
Mike Saylor, Cyber Defense Labs	Speaker At ISSA Student Chapter Meeting	N/A
Steve Austin, Raytheon	In Class Speaker	N/A
Kevin Mellot, Erase.com	In Class Speaker	N/A
Steve Austin, Raytheon	Speaker At All College Day	N/A

B. Employees: List program employees (full-time and part-time), their role, credentials, and known professional development activity since the last program review.

Table V-B: Employee Resource

Employee Name	Role in Program	Credentials	Professional Development since last Program Review

Pete Brierley	Full-Time: Networking	B.S. in Education, University of Maine PI; B.S. in Systems Analysis, University of West Florida; M.S. in Telecommunications, Southern Methodist University.
		Cisco Certified Academy Instructor (CCAI); Cisco Certified Network Associate (CCNA); Juniper Operating System (JUNIOS) Certified
			Summer 2010-High Impact Technology Exchange Conference Co-presented a seminar on Green Technology Awareness, Orlando;
			Fall 2010-Cloud Computing Conference, Santa Clara;
			Summer 2013-Cloud Computing/Big Data Conference, Cloud/Virtualization Essentials Boot camp, New York City;

Michael Harsh	Full-Time: Security	A.A.S. in Electronics, Collin College;
		B.A.A.S in Applied Technology and Performance Improvement, University of North Texas.
		
		Cisco Certified Academy Instructor (CCAI);
		Cisco Certified Network Associate (CCNA);
		Cisco Certified IT Essentials I
		
		Cybersecurity Education Consortium(CSEC) Training in: Network Security Instructor Training Workshop, Secure Electronic Commerce Instructor Training Workshop, and Enterprise Security Management Instructor Training Workshop
			Summer 2010-attended High Summer 2010 Conference;
			Summer 2010-attended High Impact technology Exchange Conference in Orlando;
			Fall 2010-Attended American Society for Industrial Security (ASIS);
			Fall 2010-Conference in Dallas;
			Spring 2011-attended the Custom Electronic Design & Installation Association Conference in Atlanta;
			Summer 2011-attended the High Impact Technology Exchange Conference in San Francisco;
			Fall 2011-presented "Staying Home Forever" at the Green IT Summit/Texas Community College Technology Fair in Plano

Stephen Willis	Full-Time: Security	B.S. in Mathematics, University of Texas at Arlington; M.S. in information Systems, Tarleton State University.
		
		Certified Information Systems Security Professional; Certified Information Systems Manager;
		Certified in Risk and Information Systems Control; Microsoft Certified System Engineer;
		Microsoft Certified System Administrator
			2010-2011-Passed the Certified Information Systems Manager certification exam; passed the Security+ certification exam; attended a Fraud Summit hosted by UT; 2011-2012-completed the requirements to be Certified in Risk and Information Systems Control; attended the UT-Dallas Executive Briefing on Cybersecurity Risks to Critical Infrastructure by the Department of Homeland Security in March

Steve Austin	Part Time: Security	B.S. in Computer Science, University of Arkansas; M.S. in Software Engineering, Southern Methodist University. Certified Information Systems Security Professional; Certified Information Systems Manager; Certified in Risk and Information Systems Control; CompTIA Security+ Certification; Microsoft Certified Solutions Expert; Microsoft Certified Solutions Associate	
Michael Saylor	Part Time: Security	AAS Mountain View College; B.S. in Information Systems, University of Texas at Arlington, M.S. in Justice Administration and Leadership, University of Texas at Dallas. Certified Information Systems Auditor; Certified Information Security Manager. Executive Director-Cyber Defense Center, University of Texas at Dallas, 2011-present; Director-Threat and Vulnerability Management Services, Price Waterhouse Coopers, 2011-2012; National Director- IT Security & Technology Risk Management, Accretive Solutions, 2004-2011; Head of Information Systems Security & Audit Compliance, VarTec Telecom/Excel Communications, 1999-2004	

C. Facilities and Resources: Describe any resources acquired in the last five years, including grants, facilities, and equipment.

Table V-C-1: Facilities Resources

Room/Office Location and Designation	Size	Type	Special Characteristics (i.e. permanent like ventilator hood)	Meets current needs: Y or N	Will meet needs for next five years: Y or N	Describe additional needs for any “N” answer in columns 5 or 6.
H134-PRC	1176 sf	Classroom	29 Computer Terminals with software allowing students to conduct hands-on labs.	Y	Y	
H241-PRC	756 sf	Conv. Lab	18 Computer Terminals outfitted with network connectivity	Y	Y	

Table V-C-2: Equipment, Supplies, Maintenance/Repairs. List all equipment required by the program that you do not consider supplies.

Current Equipment Item or Budget Amount	Meets current needs: Y or N	Will meet needs for next five years: Y or N	For any no in columns 2 or 3, justify needed equipment or budget change
N/A			

Table V-C-3: Financial Resources

Source of Funds (i.e. college budget, grant	Meets current needs: Y or N		Will meet needs for next five years: Y or N	For any no in columns 2 or 3, explain why	For any no in columns 2 or 3, identify expected source of additional funds
College Budget	Y		Y		

VI. PROGRAM PLANNING

A. Link or attach the last two CIPs. Enter name of last two CIP files here.

Exhibit: VIA1 CyberSecurity AAS Program Outcomes

Exhibit: VIA2 CyberSecurity Continuous Improvement Plan Fall 2012 and Fall 2013 Combined

B. Next CIP

1. Attach the next CIP with the data and findings on which it is based. Note: Revisions may be made to the CIP to reflect feedback from the Steering Committee or the Leadership Team. Enter name of the next CIP file here.

   Exhibit: VIB1 CyberSecurity 2014-2015 CIP Form

2. Based on the program data and the results and finding in the past two CIPs, explain how the program action plans logically flow from the data presented.
   Explain here.

   Per meeting minutes, in order to improve student understanding for the Skills Test and the Final Exam, in Fall 2012, a Comprehensive Skills Challenge Lab was implemented to review concepts in the course. By doing this, it was thought that the students will see the most critical material multiple times prior to taking the Skills Test and Final Exam. This should improve understanding for both assessments. Progress was made in terms of the Final Exam: Avg. Score (80.7 to 83.8) and the Pass Ratio (91% to 95%). However, due to three students that received zeroes, the Skills Test grades actually were lower. It is the determination of the faculty that this procedure has improved Final Exam performance. Therefore, the action planned for the next year is the implementation of a revised Challenge Lab that is based on the new Cisco CCNA curriculum.

C. Within the program's base budget, what are the plans to do one or more of the following within the next five years? Check all that apply.

- □ Increase and retain enrollment
- ☒ Increase completes
- □ Develop resources
- □ Update facilities
- □ Expand curricular opportunities
- □ Partner to increase post-graduation employment opportunities
- □ Increase transfers to related baccalaureate institutions
- □ Increase effectiveness and/or efficiency
- □ Improve student performance levels
- □ Expand services
- □ Transform services
- □ Anything else? Briefly describe
  Enter response here.

D. **What continuous improvement plans do you have,** if any, that require additional resources beyond the program’s base budget? Briefly describe what resources you will develop to secure these funds.
Enter response here.

The CIP program requires three fundamental expenditures. The three areas of need are: CyberSecurity software (some will be free and some will require funds or a donation), Biometric Devices for classroom/lab use (budgeted department funds will be used, grant funding will be sought and/or corporate donations will be requested), and the “Private Cloud Ecosystem” (corporate donations and/or grant funds will be sought).

VII. PROGRAM REVIEW REPORT PATHWAY

Completed Program Review Reports will be evaluated by the appropriate deans and Program Review Steering Committees. Following approval by the Steering Committee, Program Review Reports will be evaluated by the Leadership Team who will approve the reports for posting on the intranet. At any point prior to Intranet posting, reports may be sent back for additional development.

Leadership Team members will work with program supervisors to incorporate Program Review findings into program planning and program activity changes during the next five years.