A Proposal for a
Bachelor of Science Degree Program in
Cyber-Security at New Mexico State University

Administered by:
The College of Arts and Sciences
The College of Business
The College of Engineering

Cyber-security working group:
- Philip Braker, Engineering Technology and Surveying Engineering
- Henry Cathey, Physical Science Laboratory
- Shaun Cooper, Computer Science
- Dennis Giever, Criminal Justice
- Jay Misra, Computer Science
- James Nelson, Accounting and Information Systems
- Richard Oliver, Accounting and Information Systems
- Enrico Pontelli, Arts and Sciences
- Satish Ranade, Electrical and Computer Engineering

Contact person who can answer specific questions about the program:

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Department</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrico Pontelli</td>
<td>Dean</td>
<td>College of Arts &amp; Sciences</td>
<td><a href="mailto:epontell@nmsu.edu">epontell@nmsu.edu</a></td>
</tr>
<tr>
<td>Satyajayant Misra</td>
<td>Associate Professor</td>
<td>Dept. Computer Science</td>
<td><a href="mailto:misra@nmsu.edu">misra@nmsu.edu</a></td>
</tr>
<tr>
<td>James Nelson</td>
<td>Associate Professor</td>
<td>Dept. Accounting &amp; Inf. Systems</td>
<td><a href="mailto:jnelson@nmsu.edu">jnelson@nmsu.edu</a></td>
</tr>
</tbody>
</table>
## Contents

1 Executive Summary 4  
2 Purpose of the Program 4  
2.1 Overview of the Proposed Program 4  
2.2 Program Goals 5  
2.2.1 Vision of the BS-CSec Program 5  
2.2.2 Mission of the BS-CSec Program 5  
2.3 Academic Objectives 6  
2.4 Program Curriculum 7  
2.4.1 Admission Requirements 7  
2.4.2 Curriculum 7  
2.4.3 Learning Outcomes 8  
3 Program Justification 11  
3.1 Need for the Program 11  
3.1.1 Workforce Needs 11  
3.1.2 Student Demand 13  
3.1.3 Societal Need 13  
3.2 Relationship to NMSU Mission 13  
3.3 Relationship to Other NMSU Programs and Research Units 14  
3.4 Relationship to Programs Offered at Other New Mexico Universities 15  
3.5 Serving a Regional Need 15  
4 Clientele 15  
4.1 Student Characteristics 15  
4.1.1 Students to be Served by the Program 15  
4.1.2 Basic Entry Requirements 16  
4.1.3 Equitable Representation 16  
4.2 Projected Enrollment 16  
5 Institutional Readiness 17  
5.1 Faculty Resources 17  
5.2 Library and Curricular Resources 18  
5.3 Physical Facilities 18  
5.4 Equipment and Technology Resources 18  
5.5 Administrative Structure 18  
6 Summary of Costs and Benefits 19  
6.1 Projected Costs 19  
6.1.1 Additional faculty needed for the program 19  
6.1.2 Additional library resources needed for the program 19  
6.1.3 Additional facilities, equipment and technological resources 19  
6.2 Projected Benefits 19  
6.2.1 Financial Benefit 19  
6.2.2 Benefits to the State of New Mexico 20  
7 Assessment of Operations and Impact 20  
8 Other 21  
8.1 Accreditation 21
9 Appendices

9.1 Appendix A: Courses ......................................................... 22
9.2 Appendix B: Relevant Degree Programs at Peer Institutions ............... 25
9.3 Appendix C: Representative Programs in Other Universities ............... 26
1 Executive Summary

The proposed Bachelor of Science in Cyber-Security (BS-CSec) degree program is designed for students interested in developing expertise in the theoretical and practical aspects of cyber-security and cyber-defense. Cyber-security is an inherently interdisciplinary discipline, dealing with methods, systems, and concepts aimed at ensuring safety, resilience, and recovery of computing infrastructures. Cyber-security employs theories, methodologies, and tools drawn from many fields, within the broad areas of computer science, information systems, computer engineering, and criminal justice. The methodologies and techniques find application in a variety of domains, encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure (National Initiative for Cybersecurity Careers and Studies).

Cyber-security is a very broad and multifaceted field. The emphasis of the program will enable students to address in an analytical and scientific manner problems that are associated to enhancing safety and resilience of cyberinfrastructures, identification of safety flaws and malicious activities, and developing of recovery and impact analysis plans. To accomplish this, the BS-CSec program will provide students with a strong foundation in fundamental aspects of organization and management of computer systems and enterprise systems, security design principles, cyber-threats, information assurance and protection, and policy, legal, and societal aspects of cyber-security. The program will provide its graduates with the necessary skills to succeed in cyber-security related jobs. The presence of hands-on activities within the degree program will prepare students for success in the workplace, contributing to the workforce needs in the field of cyber-security. The theoretical and methodological foundations will prepare students to advance in their careers as well as prepare them for access to research-oriented careers and advanced degrees.

The goals of the degree program are to prepare students to fill a gap in the New Mexico’s and national workforce. This is a hands-on curriculum with opportunities for internships and culminating experiences. The program curriculum has been designed to meet the stringent academic standards of the NSA/DHS jointly sponsored CAE/CD program. BS-CSec graduates will meet an employment need in New Mexico workforce, including the pressing needs within our National laboratories (e.g., Sandia, Los Alamos) and other federal facilities (e.g., White Sands Missile Range). BS-CSec will significantly improve New Mexico’s prospect for excellence in the domain of cybersecurity and information security.

2 Purpose of the Program

2.1 Overview of the Proposed Program

According to the Bureau of Labor Statistics (BLS), employment of computer and information systems managers and administrators was projected to jump between 2008 and 2018. By 2020, it is estimated that there will be 6 million cyber-security positions worldwide, and a 1.5 million shortage in qualified specialists to fill those jobs [1]. In the U.S., this translates to a 28% cyber-security job growth through 2026, far exceeding the projected national job growth rate of 7% [2]. A recent report from Burning Glass Technologies [3], New Mexico shows a 119% growth in cyber-security jobs (with over 1,000 positions posted in 2015). Cyber-security presents an economic opportunity; however, these jobs require at least a bachelors degree [3].

NMSU is uniquely positioned to address these regional and national needs, being a research-oriented institution, with strong and growing educational and research expertise in areas relevant to cyber-security; NMSU will be able to prepare students to meet the requirements necessary to embark on challenging and rewarding cyber-security careers. Computer Science and Engineering degree programs supporting the BS-CSec program are all ABET accredited; NMSU’s proposed BS-CSec program will meet ABET cyber-security accreditation standards, which are designed to ensure graduates possess the knowledge, skills, and abilities required to meet job expectations.

From a research perspective, NMSU is the home of a number of federally funded research initiatives that have close ties to cyber-security, and will provide a solid research foundation to the BS-CSec curriculum. From an academic perspective, NMSU offers the BS-CSec graduates opportunities to matriculate into postgraduate programs offering masters and doctoral programs in cybersecurity-related areas. These
relationships and efforts enable our students to fulfill cyber-security needs in academia, government, and industry. Employment opportunities will continue to be available in both public and private sectors in areas of cyber risk and strategic analysis, vulnerability detection and assessment, cyber incident response, intelligence and investigation, networking and systems engineering. The proposed BS-CSec program will meet an under-served and growing need in industry, government and academia.

We wish to propose BS-CSec as a signature degree program for NMSU. Our primary goal is to develop a flexible interdisciplinary degree that:

- Serves students wishing to earn a degree within 120 credit hours;
- Prepares them for career opportunities or advanced education in the cyber-security field; and
- Incorporates a multidisciplinary perspective through a combination of Computer Science, Communications, Engineering, Information Systems, and Criminal Justice courses.

We propose the BS-CSec degree program as a means to address the need for higher education opportunities in this critical need area. We therefore anticipate this new degree program will provide a means to meet the needs of future students, improve enrollment across different colleges, and contribute to the advancement of the institution.

The key aim of the degree program is to address the severe shortage of skilled practitioners in the cyber-security field and address New Mexico’s workforce needs. It will prepare students to better understand, prevent, mitigate and respond to threats to cyber-security and simultaneously prepare them for optional professional certification (e.g., CompTIA Security+).

2.2 Program Goals

We propose this new degree program in response to this exploding urgent need of cyber-security professionals in the industry and government sectors. New Mexico State University is well-positioned to deliver such a degree because of existing resources—including faculty members, computing infrastructures, curriculum and courses within existing colleges and departments.

The Bachelor of Science in Cyber-Defense (BS-CSec) is designed to provide students with the necessary preparation to obtain employment in the evolving cyber-security field or to enter a course of study leading to graduate studies in cyber-security.

2.2.1 Vision of the BS-CSec Program

The BS-CSec program will be the NMSU signature interdisciplinary program to provide education and training in cyber-security and related areas, and the leading undergraduate program in cyber-security in the state of New Mexico. The degree program will be recognized regionally and nationally as a strong provider of expertise, knowledge, and discovery in the field of cyber-security. BS-CSec will be recognized for providing ongoing academic leadership in education, research, and practice necessary to develop the future workforce in computer science, information systems and information technology capable of meeting the evolving challenges of the cyber-security domain.

2.2.2 Mission of the BS-CSec Program

The Bachelor of Science in Cyber-Defense program is an interdisciplinary collaborative effort dedicated to promote learning and discovery in cyber-security and related areas of computing and information sciences. The Bachelor of Science in Cyber-Defense program will prepare computing and IT professionals who are capable of leading technological, methodological and policy changes in industry and government, both locally and nationally, with an emphasis on the protection and resilience of computing, cyber, and cyber-physical infrastructures.

BS-CSec will achieve this goal by creating a supportive and instructional learning and research environment, in which students will thrive in exploring the challenges of developing and mastering in-depth knowledge, understanding, and practical skills in the diverse areas that compose the domain of cyber-security.
The program of study will explore methodologies and technologies in analysis, prevention, deterrence, countermeasures, and recovery of information security and integrity in a global arena. Students in the BS-CSec program will have the opportunity to gain hands-on experience and participate in the design, implementation, and administration of security in a diversity of information systems in laboratory settings.

To achieve this mission, the BS-CSec program faculty will:

- Develop and maintain curriculum necessary to optimize our role of being a bridge between technology, management, and society;
- Deploy and deliver the BS-CSec curriculum adopting the most effective pedagogical practices and technologies, for both full-time and part-time students;
- Promote appropriate professional responsibility among students, through an interdisciplinary studies approach;
- Promote learning and professional excellence, to motivate the BS-CSec students to become successful cyber-security practitioners and researchers;
- Ensure the appropriate administration and coordination of course offering to meet the demand for cyber-security professionals and the development of the future New Mexico’s cyber-security workforce;
- Develop partnerships with external entities (e.g., national laboratories, industry organizations, research laboratories) to pursue joint educational and research agendas in the areas of cyber-security;
- Pursue research and funding opportunities in all areas related to cyber-security;
- Provide outreach activities to promote awareness, understanding, engagement, and preparation in the areas of cyber-security; the activities will engage
  - NMSU student organizations focused on cyber-security (e.g., sponsor teams participating in national competitions)
  - K-12 schools and
  - community organizations.
- Promote cyber-security collaborations and developments among all stake-holders at NMSU.

2.3 Academic Objectives

The primary academic purpose of this degree program is to develop professional workforce that is prepared to address the needs in the rapidly expanding cyber-security field. The students will be educated to work and excel in a variety of work settings, including private corporations, national laboratories, government and educational settings. By educating these students we will be supplying a qualified workforce to an industry which is currently looking for cost effective ways of delivering more effective security solutions to computing, enterprise and cloud-based infrastructures.

The curriculum for the BS-CSec program blends contemporary knowledge with advanced research concepts to deliver a cutting edge program. Core courses in computer network security, computer programming, host computer security, and information security provide the theoretical basis for understanding the source of vulnerabilities in computation and information systems while exposing students to state-of-the-art tools and techniques for identifying threats related to networking infrastructure, computer systems and the data and information flowing through the system. With this broad theoretical foundation, students can select courses from domain areas that provide both depth and breadth of coverage across a wide variety of topics in cyber-security.

The BS-CSec program will:

- Produce competent graduates to meet the current and future challenges in securing regional, national and global cyber-space.
The BS-CSec program will aid NMSU in gaining a leadership role in the state in the creation and delivery of knowledge in the field of cyber-security.

The BS-CSec program will provide a professionally trained workforce to industry, national laboratories, government, and academia in the domain of cyber-security. The program will meet the needs of financial, health defense, and other related organizations who are in need of skilled cyber-security graduates.

The program will help NMSU attract and retain qualified faculty with a cyber-security knowledge.

The BS-CSec program will increase enrollment of graduate students with career goals in cyber-security.

Meet industry staffing needs.

2.4 Program Curriculum

2.4.1 Admission Requirements

All students must meet the admission requirements for freshmen and/or transfer students as determined by NMSU and documented in the relevant section of the NMSU catalog.\(^1\) Students should meet the minimum of a high school cumulative GPA of 2.75, or being ranked among the top 20\% of graduating class, or an ACT composite score of 21 or SAT score of 990 (1060 for new format). Transfer students will need to meet the admission requirements as specified in the relevant section of the NMSU catalog.\(^2\) In particular, students with 30 or more college credits will need to have a cumulative GPA of at least 2.0, while students with 29 or less credits will need to meet freshmen admission requirements and have an overall GPA of at least 2.5.

2.4.2 Curriculum

All students must meet the graduation requirements for undergraduate students as determined by NMSU and also complete all Major course requirements with a grade of C- or better.

**University Requirements:**

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Category</th>
<th>Course</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Education</td>
<td>Area I</td>
<td>ENGL 111G or ENGL 111H</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ENGL 218G or ENGL 311G or ENGL 318G</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>COMM 253G or COMM 265G or HON 265G</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Area II</td>
<td>MATH 142G or MATH 235 or MATH 191G</td>
<td>3-4</td>
</tr>
<tr>
<td></td>
<td>Area III</td>
<td>CS 171G</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Additional lab science</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Areas IV and V</td>
<td>Courses per catalog</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Total</strong></td>
<td>36-37</td>
</tr>
<tr>
<td>Viewing Wider World</td>
<td>Courses per catalog</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Total</strong></td>
<td>42-43</td>
</tr>
</tbody>
</table>

**Discipline Core Requirements:**

\(^1\)https://catalogs.nmsu.edu/nmsu/essential-information-students/admissions/.

\(^2\)https://catalogs.nmsu.edu/nmsu/essential-information-students/transfer-undergraduate-students/.
### Category | Course | Credits
--- | --- | ---
Probability & Statistics | A ST 311 or STAT 371 or STAT 470 | 3
Programming | CS 111 | 4
| [CS 172 and CS 271] or [ET 262 and ET 362] or [CS 152 and CS 271] | 6-8
| CS 273 or [EE 112 and EE 212] or [ET 344 and ET 444] | 4-8
Cyber-defense and Cyber-Threats | CS 478 or BCIS 480 or [ICT 450 and ICT 457] | 3-6
Information Assurance Fundamentals | BCIS 482 | 3
Cryptography | CS 495 | 3
IT Systems, Networking, Administration | CS 480 or ET 255 or ET 464 | 3
| CS 484 or [ET 377 and ET 477] | 3-6
Policy, Legal, Ethics, Compliance | CJ 412 or ICT 339 | 3
Operating Systems Concepts | CS 474 or ET 464 | 3
Network Technologies and Protocols | CS 484 or [ET 377 and ET 477] | 3
Network Defense | BCIS 480 | 3
| CS 496 | 3
Databases | ET 458 or CS 482 | 3
Capstone course | CS 498 or A ST 498 or EE 418 or ET 441 or BCIS 498 or [TBA] or [TBA] | 3-4
Cyber Defense Capstone/Portfolio | [TBA] | 4
Cyber Defense Internship | [TBA] | 4
Total | | 54-59

Note that each student will be required to complete either a capstone course or complete an internship experience. The creation of a portfolio of activities, projects and experiences related to cyber-security will be a requirement for both tracks. Internships can be completed either within NMSU (e.g., at PSL) or within a partnering entity (e.g., a national lab, a collaborating university like UTEP).

**Discipline Elective Requirements:** At least 5 areas from the list in Tables 2 and 3. Courses can be used to meet multiple areas; some areas may require multiple courses to meet the elective area requirement. Electives should bring the total number of credits to at least 120. The list is subdivided in two parts—the first (Table 3) includes courses that are immediately available and the second (Table 2) includes courses that are part of the roadmap for ongoing development.

### 2.4.3 Learning Outcomes

Upon successful completion of this program, graduates will be well positioned to find employment in the burgeoning cyber-security industry. This will be an interdisciplinary degree drawing on faculty from various colleges (Arts and Sciences, Business, Engineering) and programs (e.g., computer science, information systems, electrical and computer engineering, information and communication technology, criminal justice). Learning outcomes for each of the individual courses will be provided by the instructors of the course, who will have the primary responsibility to see that these outcomes are achieved. The overall goal of the Bachelor of Science in Cyber-Defense program is to equip graduating students with the tools to understand, analyze and interpret cyber-physical and computing infrastructures to ensure safety, resilience and recovery. Upon completion of the BS-CSec program, students are expected to have gained the following learning outcomes:

- Apply knowledge of computing and information technologies and use software development and security analysis tools to produce effective designs and solutions for specific cyber-security problems within a variety of computing platforms and employing an approved secure systems development process model;
- Identify, analyze, and synthesize scholarly and professional literature relating to the fields of cyber-security, information security, or information assurance, to help solve specific problems and to stay abreast of the rapidly changing security context;
- Understand and be able to apply information assurance fundamentals;
- Understand and be able to apply computer forensics fundamentals;
- Assess, implement, maintain, and manage security needs of computer networks, computer infrastructures, and telecommunication systems;
- Demonstrate proficiency in secure programming.
<table>
<thead>
<tr>
<th>Category</th>
<th>Course</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithms</td>
<td>CS 372</td>
<td>4</td>
</tr>
<tr>
<td>Advanced Cryptography</td>
<td>Course Under Development</td>
<td></td>
</tr>
<tr>
<td>Advanced Networks</td>
<td>CS 584&lt;sup&gt;<em>Need Permission</em>&lt;/sup&gt;</td>
<td>3</td>
</tr>
<tr>
<td>Analog Telecommunications</td>
<td>EE 496</td>
<td>3</td>
</tr>
<tr>
<td>Data Structures</td>
<td>CS 272</td>
<td>4</td>
</tr>
<tr>
<td>Database Management Systems</td>
<td>CS 482 or ICT 458 or BCIS 475</td>
<td>3</td>
</tr>
<tr>
<td>Digital Telecommunications</td>
<td>EE 497</td>
<td>3</td>
</tr>
<tr>
<td>Digital Forensics</td>
<td>ET 339</td>
<td>3</td>
</tr>
<tr>
<td>Host Forensics</td>
<td>ET 439</td>
<td>3</td>
</tr>
<tr>
<td>Embedded Systems</td>
<td>CS 273 or EE 112</td>
<td>4</td>
</tr>
<tr>
<td>Forensics Accounting</td>
<td>ACCT 460</td>
<td>3</td>
</tr>
<tr>
<td>Theory of Computation</td>
<td>CS 370</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>CS 510</td>
<td>3</td>
</tr>
<tr>
<td>Intrusion Detection and Prevention</td>
<td>ICT 450</td>
<td>3</td>
</tr>
<tr>
<td>Life Cycle of Security</td>
<td>BCIS 482</td>
<td>3</td>
</tr>
<tr>
<td>Low level programming</td>
<td>CS 271</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>CS 273</td>
<td>4</td>
</tr>
<tr>
<td>Mobile technologies</td>
<td>CS 584&lt;sup&gt;<em>Need Permission</em>&lt;/sup&gt;</td>
<td>3</td>
</tr>
<tr>
<td>Networking and Security Administration</td>
<td>CS 484</td>
<td>3</td>
</tr>
<tr>
<td>Operating Systems Theory</td>
<td>CS 474</td>
<td>3</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>ICT 450</td>
<td>3</td>
</tr>
<tr>
<td>RF Principles</td>
<td>EE 454</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>EE 469</td>
<td>3</td>
</tr>
<tr>
<td>Secure Programming</td>
<td>CS 478</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>CS 484</td>
<td>3</td>
</tr>
<tr>
<td>Supply chain security</td>
<td>CJ 412</td>
<td>3</td>
</tr>
<tr>
<td>Systems programming</td>
<td>CS 273 or EE 112</td>
<td>4</td>
</tr>
<tr>
<td>Virtualization Technologies</td>
<td>CS 474</td>
<td>3</td>
</tr>
<tr>
<td>Vulnerability Analysis</td>
<td>ICT 450</td>
<td>3</td>
</tr>
<tr>
<td>Wireless Sensor Networks</td>
<td>CS 484&lt;sup&gt;<em>Need Permission</em>&lt;/sup&gt;</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>CS 584&lt;sup&gt;<em>Need Permission</em>&lt;/sup&gt;</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 1: Existing Elective Areas
<table>
<thead>
<tr>
<th>Category</th>
<th>Course</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithms</td>
<td>CS 372</td>
<td>4</td>
</tr>
<tr>
<td>Advanced Cryptography</td>
<td>Course Under Development</td>
<td></td>
</tr>
<tr>
<td>Advanced Networks</td>
<td>CS 584 New Course Under Planned</td>
<td>3</td>
</tr>
<tr>
<td>Analog Telecommunications</td>
<td>EE 496</td>
<td>3</td>
</tr>
<tr>
<td>Cloud Computing</td>
<td>Course Being Planned</td>
<td></td>
</tr>
<tr>
<td>Security Planning</td>
<td>Course Being Planned</td>
<td></td>
</tr>
<tr>
<td>Data Administration</td>
<td>Course Being Planned</td>
<td></td>
</tr>
<tr>
<td>Data Structures</td>
<td>CS 272</td>
<td>4</td>
</tr>
<tr>
<td>Database Management Systems</td>
<td>CS 482, ICT 457</td>
<td>3</td>
</tr>
<tr>
<td>Digital Telecommunication</td>
<td>EE 497</td>
<td>3</td>
</tr>
<tr>
<td>Digital Forensics</td>
<td>ET 339</td>
<td>3</td>
</tr>
<tr>
<td>Host Forensics</td>
<td>ET 439</td>
<td>3</td>
</tr>
<tr>
<td>Device Forensics</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Media Forensics</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Network Forensics</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Embedded Systems</td>
<td>CS 273 or EE 260</td>
<td>4</td>
</tr>
<tr>
<td>Forensics Accounting</td>
<td>ACC 460</td>
<td>3</td>
</tr>
<tr>
<td>Formal Methods</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Fraud Prevention and Management</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Hardware reverse engineering</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Hardware firmware security</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>IA architectures</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>IA Compliance</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>IA Standards</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Industrial control systems</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Theory of Computation</td>
<td>CS 370</td>
<td>4</td>
</tr>
<tr>
<td>Intrusion Detection and Prevention</td>
<td>ICT 450</td>
<td>3</td>
</tr>
<tr>
<td>Life Cycle of Security</td>
<td>BCIS 482</td>
<td>3</td>
</tr>
<tr>
<td>Low level programming</td>
<td>CS 271, CS 273</td>
<td>4</td>
</tr>
<tr>
<td>Mobile technologies</td>
<td>CS 584*</td>
<td>3</td>
</tr>
<tr>
<td>Networking and Security Administration</td>
<td>CS 484</td>
<td>3</td>
</tr>
<tr>
<td>Operating Systems Hardening</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Operating Systems Theory</td>
<td>CS 474</td>
<td>3</td>
</tr>
<tr>
<td>Cyber Operations</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>ICT 450</td>
<td>3</td>
</tr>
<tr>
<td>Quality Assurance Functional Testing</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>RF Principles</td>
<td>EE 454, EE 469</td>
<td>3</td>
</tr>
<tr>
<td>Secure Programming</td>
<td>CS 478, CS 484</td>
<td>3</td>
</tr>
<tr>
<td>Security Program Management</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Security Risk Analysis</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Software security analysis</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Software assurance</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Software reverse engineering</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Supply chain security</td>
<td>CJ 412</td>
<td>3</td>
</tr>
<tr>
<td>System certification</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Systems programming</td>
<td>CS 273</td>
<td>4</td>
</tr>
<tr>
<td>Systems Security Engineering</td>
<td>New Course Needed</td>
<td></td>
</tr>
<tr>
<td>Virtualization Technologies</td>
<td>CS 474</td>
<td>3</td>
</tr>
<tr>
<td>Vulnerability Analysis</td>
<td>ICT 450</td>
<td>3</td>
</tr>
<tr>
<td>Wireless Sensor Networks</td>
<td>CS 484, CS 584*</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 2: Roadmap Areas of Development
• Understand how physical and logical network topologies and operation apply to information security
• Research, formulate and critique security policies
• Knowledge of regional, national, and global threats to cyber systems and cyber-physical systems along with associated risk management
• Integrate knowledge from other disciplines, such as economics, management science, psychology and human factors, with their technical expertise to arrive at practical solutions that work successfully in real organizations;
• Understanding of the role of ethics and integrity for security professionals
• Ability to utilize critical thinking skills in all areas of collection and analysis
• Ability to collaborate and work effectively in teams
• Ability to enter in a lifelong learning within a cyber-security career

3 Program Justification

The Cyberspace Policy Review, published in 2009, makes the case for the creation of a national strategy to develop the workforce and expertise necessary to secure the United States cyberspace. The existing workforce in the field of cyber-security is predominantly composed of professionals with undergraduate degrees in Computer Science or Information Technology. This is because cyber-security is a relatively new major and was not available when the present workforce was in college. Given the increasing market demand for professionals with cyber-security skills, there is a clear need to develop academic programs that provide a more focused preparation in cyber-security and information assurance, thus avoiding the continuing need of supplementing traditional computer science/IT degrees with cyber-security training. Cyber-security is a multi-faceted and complex discipline, which requires its own formal education programs. The BS-CSec program has been designed to provide a strong foundation of principles of cyber-security and its applications. Since there are legal, ethical, and risk analysis aspects of cyber-security, that are integral to any solutions, the program is designed to include a strong information assurance component in the curriculum. The program provides options for students to specialize in advanced cyber-security skills through electives and special topics courses.

3.1 Need for the Program

There is extensive evidence, reported on a daily basis by news media, that cyber-security and cyber-threats are an unavoidable reality. Over 85% of banks reported losses due to cyber-attacks. Over $41 billion have been lost to one of the earliest forms of cyber-scam (the Nigerian General scam). In the last 8 months, experts have reported over 20 million new forms of malware. Experts claim that password with less than eight characters should be now considered “hopelessly inadequate” [4]. A computer connected to the internet is scanned by an attacker an average of once every 39 seconds.

The need for trained professionals to address this reality is clear. Even more important is the fact that this is one of the few IT functions that cannot be outsourced. The US remains the main international target for data breaches (e.g., Figure 15). Security is such a critical function of any organization that it has to be kept within the organization itself. It is also one of the few IT functions that is not suitable to “on-the-job training,” as the consequences of a mistake could be potentially disastrous.

3.1.1 Workforce Needs

With over 200,000 cyber-security positions available nationally, the demand far outstrips the limited supply of graduates with specialized skills in cyber-security. Recent job postings on Glassdoor.com and Indeed.com illustrate this.

According to the Bureau of Labor Statistics, information security is among the top 15 fastest growing occupations, with a growth rate (2016-26) of 28% and ranks sixth in terms of median pay (over $92,000). A survey by CIO reveals that cyber-security salaries are three times the national average [5].

Many cyber-security jobs in government require highly specialized cyber-security skills, like malware detection, cryptographic protocol design, etc., that can only be offered as part of a dedicated degree program.

Additional needs arise from the strong relationships between NMSU and military and defense installations in the region (e.g., White Sands, Fort Bliss, Holloman) and other entities associated with the Department of Homeland Security. Since the attacks of 9/11, the Department of Homeland Security and the Intelligence Community have grown exponentially. Federal security jobs grew 377% [10], with an expected growth of 42% in homeland security jobs. A Partnership for Public Service 2009 report listed the Department of Homeland Security and Department of Defense as the two agencies most likely to hire in the areas of security and protection. From 2000 until 2016, there were over 28,000 defense contracts awarded to the state of New Mexico, totaling over $15,434 million. The Department of Defense (DoD) issued, in 2008 a directive (Directive 8570) that provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions. This directive, in particular, requires 100% of DoD information assurance professional and contractors to be certified within 3 years; a recent report shows that only 30% of the approximately 90,000 affected employees have met the mandated requirements so far.

In a survey of 183 institutions offering cyber-security programs, even though the largest segment of degree programs was the master’s degree [11], one of the characteristics of the top 10 institutions offering cyber-security programs was that they offered both a bachelor’s and master’s program in cyber-security, thus demonstrating the importance of using a dedicated undergraduate degree as the ideal starting point to
build reputation and preparation in the field of cyber-security.

3.1.2 Student Demand

Many students, both domestic and international, inquire about undergraduate level offering in cyber-security at NMSU. An undergraduate level program in cyber-security would provide an opportunity for students from different but related backgrounds to specialize in cyber-security and serve the region’s and nation’s growing need for cyber-security professionals.

3.1.3 Societal Need

Recent cyber attack on companies like Equifax [9], Uber [8], and Yahoo [6] highlighted the need for increased cyber-security education and training of existing workforce and preparing a new generation of cyber-security workers ready for securing our cyberspace from intruders and attackers [7]. Many other cyber-attacks in recent times have caused extensive financial loss and inconvenience to a diversity of entities, from individual citizens to businesses and government organizations. The following facts illustrate the impact of a few of these cyber attacks.

- 53% of U.S companies expressed little to no confidence to stopping security breaches in the next 12 months.
- $445 billion is lost annually to cyber-crime and espionage across the entire world economy, according to the Center for Strategic and International Studies.
- 182,000 beneficiaries of Medicaid and the Children’s Health Insurance Program had their personal information stolen, and about 25,000 Social Security numbers were compromised in a 2012 breach of the Utah Department of Health.
- Three billion Yahoo accounts, including email, Tumblr, Flickr, were compromised in a 2013 data breach—not reported until late in 2016.
- The National Nuclear Security Administration, an arm of the Energy Department, records 10 million attempted hacks every day.
- 50 million people in North America were without power for as long as four days after an August 2003 cyber-attack to the electrical grid, according to a study by the U.S. and Canadian governments.
- Personal information of close to 150 million individuals might have been compromised as the result of a 2017 data breach that targeted Equifax, one of the largest credit agencies in the U.S.

A study by the Center for Strategic and International Studies [7] posits an annual loss to the U.S. economy of $100 to $500 billion and as many as 508,000 U.S. jobs as a result of malicious cyber activities. These losses result from cyber-attacks in six categories: the loss of intellectual property, cyber-crime, loss of business information, service disruptions, the cost of securing networks, and reputational damage to a hacked company. The Federal government has recognized the importance of cyber-security at all levels and a Comprehensive National Cyber-security Initiative (CNCI) was established by President George W. Bush in 2008 and continued by President Obama [12]. The CNCI/Initiative #8 puts specific emphasis on expanding cyber-education, to “develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees.”

3.2 Relationship to NMSU Mission

The specific goals from Vision 2020 that will benefit from the BS-CSec program are:

- Academics and Graduation:
– (KPI 1) Enrollment Growth: We expect this program to attract an audience that has not been considered so far within the state—high school graduates that have an interest in cyber-security careers, as well as transfer students (e.g., from regional community colleges) that seek this type of training. No other degree program in the state is in effect with analogous goals, while the demand for trained professionals is growing at a rapid pace. We expect this program to contribute to growth in the enrollment of the institution.

– (KPI 2) Graduate Enrollment: We propose to align the novel BS-CSec program with existing graduate programs (e.g., MS in Computer Science, MS in Electrical Engineering, MBA with Concentration in Information Systems) to facilitate transition to graduate studies upon graduation; we will explore the potential of accelerated Master’s degrees that build on BS-CSec.

– (KPI 8) STEM-H-B Degrees: BS-CSec will represent a new avenue to secure STEM degrees at NMSU.

• Diversity and Internationalization:
  – (KPI 10) Diversity: The degree program will build a recruitment plan that will promote awareness and interest towards careers in cyber-security within local K-12 schools (e.g., Las Cruces, Gadsden, Hatch), with the goal of engaging students from groups who have been traditionally underrepresented in the computing and engineering domains (e.g., students of Hispanic background, women).

• Research and Creative Activities:
  – (KPI 12) Proposals: The BS-CSec program will bring together researchers with diverse expertise but shared interest in the general area of cyber-security; we expect this to lead to new collaborations that eventually will produce new research contributions, publications, and grant proposals.
  – (KPI 13) Researcher: Two new researchers have been added to the cyber-security team in 2017 (Roopa Vishwanathan, Computer Science; Dennis Giever, Criminal Justice). Another researcher is expected to be added in Fall 2018.
  – (KPI 14) Research Funding: The BS-CSec program will bring together researchers with diverse expertise but shared interest in the general area of cyber-security; we expect this to lead to new collaborations that eventually will produce new research contributions, publications, and grant proposals.
  – (KPI 15) Publications and Creativity: The BS-CSec program will bring together researchers with diverse expertise but shared interest in the general area of cyber-security; we expect this to lead to new collaborations that eventually will produce new research contributions, publications, and grant proposals.

• Economic Development and Community Engagement:
  – (KPI 18) Community Engagement: an essential component of the BS-CSec effort will be to compose its recruitment activities with initiatives aimed at promoting awareness of issues of cyber-security within the local community. This aspect is also a requirement for the CAE/CDE certification from NSA/DHS that the program will try to secure in 2019.
  – (KPI 20) Career Placement: The outstanding job opportunities in the field of cyber-security will guarantee that our graduates will have access to excellent and rewarding careers.

3.3 Relationship to Other NMSU Programs and Research Units

The proposed BS-CSec degree program does not duplicate any existing program at NMSU. The program overlaps some its requirements with the following programs:

• Bachelor of Science in Computer Science—this program covers similar background in terms of programming and understanding of computing systems, but does not have a specific emphasis on security;
Bachelor of Business Administration/Information Systems—this program provides an emphasis on business information systems, with introductory concepts in digital forensics;

- Bachelor of Information and Communication Technology—this program covers some of the applied aspects of cyber-security, placing emphasis on the deployment and management of information systems;

- Bachelor of Science in Engineering Technology—this program provides some foundations of software development and communication infrastructures.

Furthermore, the program nicely complements and integrates with the cyber-security activities that are ongoing within the Physical Science Laboratory (PSL). PSL offers the unique interface to provide practical real world training opportunities for NMSU students in the cyber-security and Information Assurance (IA)/Information Operations (IO) through current ongoing customer contracts.

### 3.4 Relationship to Programs Offered at Other New Mexico Universities

The proposed BS-CSec program does not duplicate an existing Bachelor degree program offered by another university in New Mexico.

- University of New Mexico: the institution does not offer a comparable undergraduate degree; the institution offers a Master’s degree in Information Systems and Assurance (in the Business College);

- New Mexico Institute of Mining and Technology: the institution offers a Bachelor in Information Technology with some coverage of secure systems, risk analysis and protection;

- New Mexico Highlands University: the institution does not appear to offer any emphasis on cyber-security in any of its programs;

- Eastern New Mexico University: the institution offers a Bachelor of Business Administration with emphasis in Information Systems, which covers some issues of security;

- Northern New Mexico College: the Bachelor of Engineering in Information Technology includes one course in information assurance;

### 3.5 Serving a Regional Need

The BD-CD program fills a regional gap that can be clearly gained from the preceding discussion. The long-standing history of New Mexico in the area of defense and the dominant role in cyber-security gained by entities like PSL, Sandia, Los Alamos, ARL, support the need for the development of a program like BS-CSec, in order to supply professional workforce and advance New Mexico’s role of leadership in the area. As can be seen in our review of existing programs (section 3.4), there are no comparable undergraduate programs offered in the state at the present time. Furthermore, the analysis of programs at our peer institutions (Appendix B) indicates that, while there is a growing interest and educational commitment to cyber-security, there is no undergraduate organized curriculum offered at such institutions that specifically focuses on cyber-security and related areas.

### 4 Clientele

#### 4.1 Student Characteristics

##### 4.1.1 Students to be Served by the Program

The BS-CSec program will be available to all interested individuals who successfully meet the NMSU admissions criteria established for the program. The program will be open to full-time and part-time students. All applicants must be high school graduates and take an admissions test to establish reading, writing, and math abilities. No restriction will be made regarding race, creed, gender or age. The program will draw students primarily from New Mexico and West Texas. The opportunities for employment in the field will
be both regional (New Mexico) as well as national. The program also will appeal to people already in the workforce who have experience in cyber-security and are seeking additional training so they can increase their skill level and become prepared for additional job opportunities in these growing career fields.

4.1.2 Basic Entry Requirements

Admission requirements have been stated in an earlier section of this document. Nevertheless, the degree requirements would suggest incoming students to meet the following additional requirements:

- Have completed Trigonometry and Pre-calculus by the time of entrance—i.e., have a preparation in mathematics equivalent to MATH 190G;
- Do not have any developmental English prerequisites—i.e., be ready to enter ENGL 111G

4.1.3 Equitable Representation

We will market the program broadly to help ensure diverse cohorts of students. Given the diversity of students in the school systems that feed into our undergraduate programs (e.g., Las Cruces Public Schools, Gadsden Independent Schools), we will encourage students from groups that are traditionally underrepresented in cyber-security to participate in the BS-CSec program. These groups include students of Hispanic heritage and women. We will build on and expand our existing K-12 outreach programs that have been specifically designed to serve these student populations (e.g., the Computing Alliance of Hispanic Serving Institutions, the Young Women in Computing Program).

The Department of Computer Science has a long-standing commitment to serve a very diverse student population. NMSU Computer Science has launched and supports a wide range of initiatives to promote recruitment, training, and retention of students from traditionally under-represented backgrounds. These projects include outreach programs (e.g., summer camps for middle-school and high-school students), training and motivational events (e.g., a year-around set of activities for cohorts of high school women), and solid links with local high schools and community colleges, and collaborations with Hispanic-Serving Institutions across the nation (e.g., NMSU is one of the leading institutions in the Computing Alliance of Hispanic Serving Institutions).

It is important to underline the importance of the development of this type of program in a region like New Mexico. The field of computing in general, and cyber-security in particular, is still witnessing a severe under-representation of women and of students from traditionally under-represented ethnic groups. In particular, less than 18% of undergraduate computing degrees are of women; 7.5% of undergraduate computing degrees are awarded to Hispanic students (parity would be 17%) [13]. The diversity in the population of New Mexico, and in particular the diversity offered by our local school systems, offer an untapped pool of talent on which to build a successful and strong program, laying the foundations for bringing New Mexico to the forefront of training in cyber-security.

4.2 Projected Enrollment

The following table (Table 3) provides an estimate of enrollment for the BS-CSec program.

<table>
<thead>
<tr>
<th>Year</th>
<th>Incoming Students</th>
<th>Projected Total Enrollment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year 1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Year 2</td>
<td>10</td>
<td>18</td>
</tr>
<tr>
<td>Year 3</td>
<td>15</td>
<td>30</td>
</tr>
<tr>
<td>Year 4</td>
<td>15</td>
<td>42</td>
</tr>
<tr>
<td>Year 5</td>
<td>25</td>
<td>50</td>
</tr>
<tr>
<td>Year 6</td>
<td>25</td>
<td>42</td>
</tr>
</tbody>
</table>

Table 3: Project Enrollment
These enrollment projections are conservative, providing the least optimistic financial impact scenario for the BS-CSec program. Actual enrollment for BS-CSec is expected to be larger, depending on the degree of support provided to a strong roll-out of the program and establishment of a positive reputation among local schools and communities.

5 Institutional Readiness

5.1 Faculty Resources

The institution has already an adequate pool of qualified researchers and educators to meet the needs of the proposed degree program. The following is a description of the faculty members who have participated in the development of this proposal or who have been identified as potential contributors to the BS-CSec program:

- Enrico Pontelli, Computer Science/Arts & Sciences, Regents Professor and Dean;
- Satyajayant Misra, Computer Science, Associate Professor;
- Roopa Vishwanathan, Computer Science, Assistant Professor;
- Huiping Cao, Computer Science, Associate Professor;
- Jonathan Cook, Computer Science, Professor;
- Shaun Cooper, Computer Science, College Assistant Professor;
- Mai Zheng, Computer Science, Assistant Professor;
- Richard Oliver, Accounting & Information Systems, Professor;
- James Nelson, Accounting & Information Systems, Associate Professor;
- Satish Ranade, Electrical & Computer Engineering, Professor and Department Head;
- Abdel-Hameed S Badawy, Electrical and Computer Engineering, Assistant Professor;
- Hong Huang, Electrical and Computer Engineering, Associate Professor;
- Phillip De Leon, Electrical and Computer Engineering, Professor and Associate Dean;
- Philip Braker, Engineering Technology, Assistant Professor;
- Dennis Giever, Criminal Justice, Professor and Department Head;

Although cyber-security and cyber-defense have exploded most rapidly in the business and government sectors, cyber-security is a pervasive discipline, and therefore it is crucial that the proposed program is interdisciplinary in scope. It is important that its delivery and administration is shared among colleges and includes faculty with relevant experience who represent the different facets of this field and the different organization types that the degree serves. Current leaders will also be included as guest lecturers or speakers.

In addition, PSL offers staff trained in a variety of aspects of cyber-security. We will build on this expertise by engaging PSL staff in course content (e.g., as guest lecturers, as providers of course projects). We envision PSL as one of the entities that can provide students with the required internship opportunity.
5.2 Library and Curricular Resources

The curriculum for the BS-CSec program builds primarily on courses that are already in place and successfully offered. All students already taking these courses have found adequate support with the current materials provided by the library and by the fast-growing publicly accessible repositories of online materials. Nonetheless, a request to the library to evaluate current resources was made. The library reported fewer resources/funds have substantially decreased over the years. Even with fewer resources, we believe that the total holdings listed in the library’s report should be sufficient for a small cohort of students. In addition, with membership in the Association for Computing Machinery (ACM), all faculty and student members would have access to the primary journals and conferences in the field as part of their membership.

5.3 Physical Facilities

No new facilities are required to support the offering of this program. The existing laboratories (e.g., with the Department of Computer Science and the Department of Electrical and Computer Engineering) will be sufficient to support the proposed curriculum.

5.4 Equipment and Technology Resources

No new equipment is required to support the offering of this program. Equipment currently available at the participating departments within NMSU is sufficient to fully support the launch and initial phases of this program. As the program grows, it is expected that new equipment/funds will be required to ensure adequacy of virtual laboratory resources both within the NMSU and commercially (e.g., Amazon EC2) respectively.

5.5 Administrative Structure

We propose to establish an administrative organization for the proposed interdisciplinary program that will ensure that the three Colleges participating in the BS-CSec program have representation and voice in the management and evolution of the program (see Figure 2). The BS-CSec program will be jointly managed by the College of Arts & Sciences, the College of Business, and the College of Engineering.

Figure 1 shows a proposed organization for the administrative structure of the BS-CSec program. The BS-CSec program will have a director, appointed by the three Deans. The Director will receive a one-course release to enable the duties associated with the program, and the course release will be managed by the College from where the Director comes from. The School Director reports to the three Deans.

The School will have a steering committee composed of faculty members from the core departments providing courses to the program (Computer Science, Engineering Technology, Accounting and Information Systems, Electrical and Computer Engineering). The membership to the committee will be approved by the Deans of the three colleges. The steering committee assists the director in decisions concerning curricular structure and evolution of curriculum, advertisement and recruitment of students, and help with recruitment of new faculty members.

![Figure 2: Proposed Administrative Structure](image-url)
6 Summary of Costs and Benefits

6.1 Projected Costs

6.1.1 Additional faculty needed for the program

We expect to have a sufficient minimal number of faculty members if the current search being conducted in the Department of Electrical and Computer Engineering is successful. The limited number of elective areas that we can currently adequately cover would suggest the need of one additional faculty line, probably with expertise in the software development aspects of cyber-security, to be needed in the near future (i.e., within two years from the launch of the program).

6.1.2 Additional library resources needed for the program

The initial launch of the program will not require any additional library resources. Due to the speed of evolution of the field, professionals in cyber-security tend to rely predominantly on open-source and open-access materials and documents.

6.1.3 Additional facilities, equipment and technological resources

An immediate facility need that we will have to address within the first two years of activities of the program is the establishment of at least one additional laboratory dedicated to cyber-security training. The cost is expected to be limited—the laboratory can be equipped with older computers and with a dedicated network. The estimated cost of a 20-seat laboratory of this type is:

- 20 desktops, $460 each, total $9,200
- Networking (switches, cabling): $3,000
- Instructor workstation: $2,100
- Supplies: $1,500
- Furniture (Desks, chairs): $9,000

The college of Arts & Sciences is committed to invest to invest funds to establish this facility over a 2-year period.

6.2 Projected Benefits

6.2.1 Financial Benefit

The following table provides an estimate of tuitions generated by the program according to the projected enrollment, assuming full-time students with a 15-credit per semester load.
<table>
<thead>
<tr>
<th>Year</th>
<th>Type</th>
<th>Description</th>
<th>Estimated</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cost</td>
<td>Graduate Assistant</td>
<td>$17,770</td>
<td>($17,770)</td>
</tr>
<tr>
<td></td>
<td>Revenue</td>
<td>Tuitions &amp; Fees, 10 students</td>
<td>$35,610</td>
<td>$35,610</td>
</tr>
<tr>
<td>2</td>
<td>Cost</td>
<td>Graduate Assistant</td>
<td>$17,770</td>
<td>($17,770)</td>
</tr>
<tr>
<td></td>
<td>Revenue</td>
<td>Tuitions &amp; Fees, 18 students</td>
<td>$64,098</td>
<td>$64,098</td>
</tr>
<tr>
<td>3</td>
<td>Cost</td>
<td>Graduate Assistant</td>
<td>$17,770</td>
<td>($17,770)</td>
</tr>
<tr>
<td></td>
<td>Cost</td>
<td>New Laboratory</td>
<td>$24,800</td>
<td>($24,800)</td>
</tr>
<tr>
<td></td>
<td>Revenue*</td>
<td>Tuitions &amp; Fees, 30 students</td>
<td>$108,967</td>
<td>$108,967</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* estimated 2% tuition&amp;fees increase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Cost</td>
<td>Graduate Assistant</td>
<td>$17,770</td>
<td>($17,770)</td>
</tr>
<tr>
<td></td>
<td>Revenue</td>
<td>Tuitions &amp; Fees, 42 students</td>
<td>$152,553</td>
<td>$152,553</td>
</tr>
<tr>
<td>5</td>
<td>Cost</td>
<td>Graduate Assistant</td>
<td>$17,770</td>
<td>($17,770)</td>
</tr>
<tr>
<td></td>
<td>Revenue</td>
<td>Tuitions &amp; Fees, 50 students</td>
<td>$181,611</td>
<td>$181,611</td>
</tr>
<tr>
<td>6</td>
<td>Cost</td>
<td>Graduate Assistant</td>
<td>$17,770</td>
<td>($17,770)</td>
</tr>
<tr>
<td></td>
<td>Revenue</td>
<td>Tuitions &amp; Fees, 50 students</td>
<td>$181,611</td>
<td>$181,611</td>
</tr>
</tbody>
</table>

### 6.2.2 Benefits to the State of New Mexico

The benefits to the state of New Mexico from the presence of the BS-CSec program are extensive. First of all, there is a growing demand of trained cyber-security professionals by a variety of industries and contractors in the state; Indeed.com currently lists 189 posted jobs, with an average salary of $94,794. The demand is also high due to the presence of federal facilities and national laboratories in the state. Sandia National Laboratories is at the forefront in research and development in the domain of cyber-security; Army Research Laboratory has facilities at White Sands and provides excellent opportunities for collaboration in the area of cyber-security, especially through its ARL South Open Campus initiative.

### 7 Assessment of Operations and Impact

As all academic programs at NMSU, we expect BS-CSec to be formally reviewed every five years, through the development of a self-study and an external evaluation. Additional assessment will derive from the reporting requirements imposed by NSA/DHS, which will become effective as soon as the institution receives CAE/CDE certification. NSA/DHS requires a formal assessment of the program every five years. Students completing the BS-CSec program are required to complete either a thesis or a capstone project, which require multiple reviewers among the faculty involved in the program. In both cases, the course objectives will encompass the student learning outcomes for the program.

Students are required to complete a cyber-security Portfolio in addition to those courses defined within the program. Students construct a portfolio from the projects completed as part of the major course requirements portion of the program. The portfolio is intended to enable assessment of those learning outcomes that are best assessed in an integrative fashion, spanning all of the students course work and therefore reflects overall academic growth.

The program review will benefit from interaction with industry and government. Examples of such interaction include presence of representatives from national labs (e.g., Sandia) on the BS-CSec advisory board, student involvement in industry/government sponsored cyber-security internships, and frequent industry/government guest speakers.

Another key part of the formative assessment will be to evaluate the alignment of the BS-CSec curriculum with community colleges (e.g., DACC). The analysis will assess the successful connections made, the challenges encountered, and the recommendations for making the program even more accessible to students throughout New Mexico.

The results of the evaluation will be reported to the Executive Vice President and Provost and to the program advisory board.
8 Other

8.1 Accreditation

There is not yet an accrediting body for cybersecurity degree programs. ABET is currently working on a set of requirements to provide accreditation of cyber-security computing programs—a preliminary list of requirements is available for comments and a vote on the requirements is expected by the end of 2018. The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cyber-Defense (CAE/CDE) program. The goal of this program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in information assurance (IA) and cyber-defense (CD), and producing a growing number of professionals with CD expertise in various disciplines. Designation as a CAE/CD is valid for five academic years, after which the school must successfully reapply in order to retain its CAE designation. The plan is for NMSU to apply for such designation in January 2019. The outline of courses presented in section 2.4 provides an excellent snapshot of what will likely be included in the accreditation requirements. These classes will position NMSU to fulfill the likely national requirements, and as needed, will be modified to address any additional needs identified.
Appendices

Appendix A: Courses

- ENGL 111G - Skills and methods used in writing university-level essays. 4 credits
- ENGL 111H - Individualized assignments and independent study. 4 credits
- ENGL 218G - Effective writing for courses and careers in sciences, engineering, and agriculture. Strategies for understanding and presenting technical information for various purposes to various audiences. 3 credits
- ENGL 318G - Theory and practice of writing in technical and professional fields, individualized to each student's field. Emphasizes efficient writing processes and effective written products. 3 credits
- COMM 265G - Study and practice of interpersonal, small group, and presentational skills essential to effective social, business, and professional interaction. 3 credits
- HON 265G - Study and practice of interpersonal, small group, and presentational skills essential to effective social, business, and professional interaction. 3 credits
- MATH 142G - Review of functions. Derivatives, exponential and logarithmic functions, antiderivatives and indefinite integrals, basic ordinary differential equations and growth models, with an emphasis on applications. Includes a significant writing component. 3 credits
- MATH 191G - Limits and continuity, theory and computation of derivatives, applications of derivatives, extreme values, critical points, derivative tests, L'Hôpital's Rule. 4 credits
- C S 111 - This course provides a broad and exciting introduction to the field of computer science and the impact that computation has today on every aspect of life. It focuses on exploring computing as a creative activity and investigates the key foundations of computing: abstraction, data, algorithms, and programming. It looks into how connectivity and the Internet have revolutionized computing and demonstrates the global impact that computing has achieved, and it reveals how a new student in computer science might become part of the computing future. 4 credits
- CS 171G - Computers are now used widely in all area of modern life. This course provides understanding of the theoretical and practical foundations for how computers work, and provides practical application and programming experience in using computers to solve problems efficiently and effectively. The course covers broad aspects of the hardware, software, and mathematical basis of computers. Weekly labs stress using computers to investigate and report on data-intensive scientific problems. Practical experience in major software applications includes an introduction to programming, word processing, spreadsheets, databases, presentations, and Internet applications. 4 credits
- C S 172 - Computational problem solving; problem analysis; implementation of algorithms. Recursive structures and algorithms. 4 credits
- C S 271 - Introduction to problem analysis and problem solving in the object-oriented paradigm. Practical introduction to implementing solutions in the C++ language. Hands-on experience with useful development tools. 4 credits
- C S 272 - Design, implementation, use of fundamental abstract data types and their algorithms: lists, stacks, queues, deques, trees; imperative and declarative programming. Internal sorting; time and space efficiency of algorithms. 4 credits
- C S 273 - Computer structure, instruction execution, addressing techniques; programming in machine and assembly languages. 4 credits
- C S 370 - Methods, principles, and tools for programming language processor design; basics of formal language theory (finite automata, regular expressions, context-free grammars); development of compiler components. 4 credits
• C S 372 - Introduction to efficient data structure and algorithm design. Order notation and asymptotic run-time of algorithms. Recurrence relations and solutions. Abstract data type dynamic set and red-black trees. Classic algorithm design paradigms: divide-and-conquer, dynamic programming, greedy algorithms. 4 credits

• C S 474 - Operating system principles and structures, and interactions with architectures. 3 credits

• C S 478 - Introduction to the art and science of computer security. Fundamentals of computer security including elementary cryptography, authentication and access control, security threats, attacks, detection and prevention in application software, operating systems, networks and databases. 3 credits

• C S 479 - Topic announced in the Schedule of Classes. May be repeated if subtitle is different. Not for C S graduate students. 1-6 credits

• C S 480 - Basic system administration for Linux environments. Topics include user management, file systems, security, backups, system monitoring, kernel configuration and other relevant aspects of system administration. 3 credits

• C S 482 - Database design and implementation; models of database management systems; privacy, security, protection, recovery. 3 credits

• C S 484 - Fundamental concepts of computer communication networks: layered network architecture, network components, protocol stack and service. Example of application, transport, network and data link layers, protocols primarily drawn from the Internet (TCP, UDP, and IP) protocol multimedia networks; network management and security. 3 credits

• C S 496 - Cloud and Edge Computing: the course presents a top-down view of cloud computing, from applications and administration to programming and infrastructure. Its main focus is on the concepts of networking and parallel programming for cloud computing and large scale distributed systems which form the cloud infrastructure. The topics include: overview of cloud computing, cloud systems, parallel processing in the cloud, distributed storage systems, virtualization, security in the cloud, and multicore operating systems. Students will study state-of-the-art approaches to cloud computing followed by large cloud corporations, namely Google, Amazon, Microsoft, and Yahoo. Students will also apply what they learn through project developments using Amazon Web Services. 3 credits

• C S 584 - Advanced topics in computer networks. Covers advanced topics in networking, with emphasis on wireless, and IP networks. 3 credits

• A ST 311 - Techniques for describing and analyzing economic and biological data; estimation, hypothesis testing, regression and correlation; basic concepts of statistical inference. 3 credits

• STAT 371 - Modern probability and statistics with applications to the engineering sciences. 3 credits

• E T 262 - An introduction to computer programming concepts as applied to engineering technology. Includes basic logic design, algorithm development, debugging and documentation. History and use of computers and their impact on society. 3 credits

• E T 339 - Introduction to the skills required to perform digital forensics and incident response on Windows operating systems. Topics include: live response, evidence acquisition, Windows operating system artifacts, documentation and reporting. 3 credits

• E T 362 - A continuation of topics from E T 262 that are directed toward more advanced software development. Topics include problem analysis, object oriented, structured logic, and development concepts. 3 credits

• E T 439 - Advanced topics in digital forensics and incident response on Windows, Linux and Mac OS X and mobile devices. Topics include: Memory analysis, registry analysis, timeline analysis, malware analysis, Linux and Mac artifacts, mobile device forensics. 3 credits
• E T 463 - Advanced Linux Includes installation and maintenance of Unix/Linux/Windows versions of Python. Use of Python to solve numerous engineering problems including video and audio. Image manipulation. Using PostScript for image and typesetting development. Integration of C programming with Python.

• E T 464 - Learn about configuration and maintenance of Microsoft Windows Server and related services such as DHCP, DNS, Failover Clusters, Active Directory, Group Policy, File Sharing, Microsoft SQL server, Microsoft Exchange Server, IIS, Network Load Balancing, Backups, Remote Administration, PowerShell scripting and more. 3 credits

• BCIS 480 - Introduction to securing network-based applications from internal and external threats. Fundamentals of network security, including TCP/IP, firewalls, intrusion detection, and vulnerability. 3 credits

• BCIS 482 - Provides management overview of information security and thorough examination of administration of information security. Surveys field of information security including planning, policy and programs, protection and people relative to information security. 3 credits

• ICT 339 - Introduction to the skills required to perform digital forensics and incident response on Windows operating systems. Topics include: live response, evidence acquisition, Windows operating system artifacts, documentation and reporting. 3 credits

• ICT 450 - Ethical Hacking and Penetration testing techniques. 3 credits

• E E 454 - Basic antenna analysis and design. Fundamental antenna concepts and radiation integrals. Study of wire antennas, aperture antennas, arrays, reflectors, and broadband antennas. 3 credits

• ICT 457 - This course provides an overview of security challenges and strategies of countermeasure in the information systems environment. Topics include definition of terms, concepts, elements, and goals incorporating industry standards and practices with a focus on availability, vulnerability, integrity and confidentiality aspects of information systems. 3 credits

• E T 458 - MySQL and PHP. Data conversion using PHP, mysql and Python. Methods of transferring data from electronic boards and data feeds, into databases. Use of SQL in java programming. Remote programming of computers for running database systems in a mixed OS environment. Generation of web pages directly from Database queries. 3 credits

• E E 459 - Introduction to the design and performance analysis of communications networks with major emphasis on the Internet and different types of wireless networks. Covers network architectures, protocols, standards and technologies; design and implementation of networks; networks applications for data, audio and video; performance analysis. 3 credits

• C J 412 - Private and public responses to security problems, including employee theft, perimeter security, and domestic or foreign terrorism; reviews related law and management practices. 3 credits

• E E 112 - Introduction to programming through microcontroller-based projects. Extensive practice in writing computer programs to solve engineering problems with microcontrollers, sensors, and other peripheral devices. 4 credits

• E E 212 - Introduction to computer architecture and performance analysis techniques. Design and optimization of systems such as personal mobile devices and cloud computing systems. 4 credits

• E E 496 - Introduction to the analysis of signals in the frequency and time domains. A study of baseband digital transmission systems and digital/analog RF transmission systems. Introduction to telecom systems as well as satellite systems. 4 credits

• E E 497 - Techniques for transmitting digital data over commercial networks. Topics include baseband and bandpass data transmission and synchronization techniques. 3 credits
• ACCT 460 - Covers business fraud as it is occurring in American society. Emphasis is on occupational fraud and financial statement fraud. Examines various types of fraud, its symptoms and effective investigation techniques. Effective fraud prevention measures are discussed throughout the course. Emphasizes case studies and the application of principles to actual fraud cases. 3 credits

9.2 Appendix B: Relevant Degree Programs at Peer Institutions

University of Arizona: UA offers a cybersecurity certificate in its UA South campus—18 credits focused on fundamentals and applications. UA main campus offers an online Master’s degree, composed of 33 credits with emphasis on foundations and data mining applications.

Colorado State University: CSU offers an undergraduate certificate in cybersecurity, with emphasis on applied administration aspects. The institution offers an online MS degree in Telecommunication with a network security track.

University of Idaho: the institution runs an online MS degree in Computer Science with a track on security.

Iowa State University: the institution offers an online Master of Engineering degree in Information Assurance. A face-to-face Master of Science in Information Assurance is available as well. No undergraduate degree programs in cybersecurity are provided.

Kansas State University: the institution appears to offer only a concentration in unmanned aircraft systems cyber security as part of the Professional Master of Technology. No undergraduate cybersecurity programs are offered.

Montana State University: the institution does not appear to offer any formal degree program in cybersecurity.

University of Nevada-Reno: the institution has been very active in the area of cyber-security. It established a center, which launched an undergraduate minor (18 credits) and a graduate certificate (12 credits).

University of Nebraska-Lincoln: the institution does not appear to offer any formal degree program in cyber-security.

University of North Texas: the only formal program in cyber-security is an undergraduate certificate (18 credits).

Oklahoma State University: the institution provides an undergraduate degree in management information system with an option in information assurance, mostly focused on issues of information assurance and more limited coverage of other aspects of cyber-security. The unit offers also a Master of Science in Information Assurance, with an heavy applied curriculum.

Oregon State University: the institution does not offer a formal degree program in cyber-security.

University of Texas at El Paso: in spite of great activity in the area of cyber-security, the only formal degree available is a graduate certificate (15 credits).

Texas Tech University: the institution is the home of the Center for the Science and Engineering of Cyber Security, which supports a graduate certificate in cybersecurity for critical infrastructures. No undergraduate degree programs appear to be available.
Utah State University: the institution does not appear to provide any formal degree program in cyber-security.

Washington State University: the institution does not offer any dedicated degree program in cyber-security—they offer collections of courses within the graduate and undergraduate Computer Science programs.

University of Wyoming: the institution does not offer any dedicated degree program in cyber-security.

9.3 Appendix C: Representative Programs in Other Universities

Examples of other public and private non-profit universities that offer related programs include the following:

- Norwich University (Bachelor of Science - Computer Security & Information Assurance)
- Champlain College (Bachelor of Science in Computer Networking & Cybersecurity)
- Rochester Institute of Technology (Bachelor of Science in Computing Security)
- Towson University (Bachelor of Science in Computer Science with a Computer Security track and a Master of Science in Computer Science with a Computer Security track)
- Drexel University (Bachelor of Science in Computing & Security Technology)
- Kennesaw State University (Bachelor of Business Administration - Information Security and Assurance)
- High Point University (Bachelor of Science in Cybersecurity and Privacy)
References


