DEPARTMENT OF
HIGHER EDUCATION &
WORKFORCE DEVELOPMENT

New Program Report

Date Submitted:
02/10/2020

Institution

Central Methodist University

Site Information

Implementation Date:
8/1/2020 12:00:00 AM

Added Site(s):

Selected Site(s):

CIP Information

CIP Code:
110101

CIP Description:
A general program that focuses on computing, computer science, and information science and systems. Such programs are undifferentiated as to title and content and are not to be confused with specific programs in computer science, information science, or related support services.

CIP Program Title:
Computer and Information Sciences, General

Institution Program Title:
Cybersecurity

Degree Level/Type

Degree Level:
Bachelor's Degree

Degree Type:
Bachelor of Science

Options Added:

Collaborative Program:
N

Mode of Delivery

Current Mode of Delivery

Online

Student Preparation

Special Admissions Procedure or Student Qualifications required:
Once candidates meet the qualification for Admission to the Central Methodist University, there will be no special procedures or student qualifications required, outside of general requirements noted in the program structure.

New Program Report

Specific Population Characteristics to be served:
n/a

Faculty Characteristics

Special Requirements for Assignment of Teaching for this Degree/Certificate:
Master's Degree or higher in similar field.

Estimate Percentage of Credit Hours that will be assigned to full time faculty:
60% of cybersecurity will be assigned to full time faculty, 70% of criminal justice will be assigned to full time faculty.

Expectations for professional activities, special student contact, teaching/learning innovation:
No special expectations for professional activities.

Student Enrollment Projections Year One-Five

Year 1	**Full Time:** 5	**Part Time:** 5	
Year 2	**Full Time:** 10	**Part Time:** 10	
Year 3	**Full Time:** 15	**Part Time:** 15	**Number of Graduates:** 10
Year 4	**Full Time:** 15	**Part Time:** 15	
Year 5	**Full Time:** 25	**Part Time:** 10	**Number of Graduates:** 25

Percentage Statement:
n/a

Program Accreditation

Institutional Plans for Accreditation:
At this time, there are no plans for accreditation but Central Methodist University strives to develop a Cyber program that blends with an already strong Criminal Justice program that also meets NSA/DHS Center for Academic Excellence, Cyber Defense track, requirements.

Program Structure

Total Credits:
120

Residency Requirements:
Candidates for a baccalaureate degree must complete at least 30 of the last 36 hours of credit in residence at Central Methodist University.

General Education Total Credits:
42

Major Requirements Total Credits:
30

Course(s) Added

COURSE NUMBER	CREDITS	COURSE TITLE
CYB320	3	Cybersecurity Risk, Compliance, and Threats

AC313	3	Fraud Examination
CYB310	3	Cybersecurity Law and Policy
CJ202	3	Criminal Law
CYB205	3	Network Essentials
CYB330	3	Cybersecurity Operations
CJ270	3	Criminal Procedure
CYB350	3	Cyber Crime
CYB101	3	Introduction to Cybersecurity
CJ100	3	Introduction to Criminal Justice
CYB340	3	Cyber Incidents Response and Forensics

Free Elective Credits:
0

Internship or other Capstone Experience:
Central Methodist University will embed capstone in 300-level cybersecurity courses.

Assurances

I certify that the program will not unnecessarily duplicate an existing program within the geographically applicable area.

I certify that the program will build upon existing programs and faculty expertise.

I certify that the institution has conducted research on the feasibility of the proposal and it is likely the program will be successful. Institutions' decision to implement a program shall be based upon demand and/or need for the program in terms of meeting present and future needs of the locale, state, and nation based upon societal needs, and/or student needs.

Contact Information

First and Last Name: Deborah
Dixon

Email: ddegan@centralmethodist.edu

Phone: 660-264-0025

Central Methodist University
New Academic Program Proposal – Cybersecurity

Program Goals/Outcomes

Students with a Major in Cybersecurity will be able to recognize, discuss and explain information security principles and how those information principles apply to industry.

- Students will be able to demonstrate the information security risk analysis and describe/apply various information security tools.
- Students will be able to compare and contrast the domestic and international information security issues and legal issues.
- Students will develop technical and administrative skills and apply them to the information security industry.

Central Methodist Strategy

Develop a Cyber program that blends with an already strong Criminal Justice program that also meets NSA/DHS Center for Academic Excellence, Cyber Defense track, requirements.

Recommended CAE alignment (Cyber Defense Track):

Cyber Investigations

Knowledge Units (KU)s necessary to impart the necessary skills and abilities for performing technical analyses of computer incidents and intrusions to determine source, infiltration path, mechanism, system modifications and effects, damages, exfiltration path, data infiltrated, and residual effects.

To complete this specialization area, students must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- Technical Core KUs
  - Basic Networking
- Non-Technical Core KUs or Cyber Threats
  - Policy, Legal, Ethics, and Compliance
  - Security Risk Analysis
- Optional KUs
  - Cyber Crime

    - Cybersecurity Ethics
    - Forensic Accounting
    - Fraud Prevention and Management
    - IA Compliance
    - Privacy

Draft BS Cyber Security Major Requirements (30 Hours)

CMU Cyber Core (27 hours)			
Course Name	**Hours**	**Status**	**Alignment**
CJ100- Introduction to Criminal Justice	3	Existing	CAE Support
CJ202- Criminal Law	3	Existing	CAE Support
CJ270- Criminal Procedure	3	Existing	CAE Support
CYB101: Intro to Cybersecurity	3	New	CompTIA Security+
CYB205: Network Essentials	3	New	Meets Req CAE KU CompTIA Network+
CYB310: Cybersecurity Law and Policy	3	New	Meets Req CAE KU
CYB320: Cybersecurity Risk, Compliance, and Threats	3	New	Meets Req CAE KU
CYB330: Cyber Security Operations	3	New	CompTIA PenTest+
CYB340: Cyber Incident Response and Forensics	3	New	CompTIA CySA+
CMU Cyber Electives			
AC313- Fraud Examination	3	Existing	CAE Optional KU
CYB350: Cyber Crime	3	New	CAE Optional KU

Result

1. Alignment to apply for NSA/DHS Center for Academic Excellence, Cyber Defense
    - Technical Core KUs

    - Basic Networking (Met by CYBXXX: Network Essentials)
- Non-Technical Core KUs o Cyber Threats
    - Policy, Legal, Ethics, and Compliance (Met by CYBXXX: Cybersecurity Law and Policy)
    - Security Risk Analysis (Met by CYBXXX: Cybersecurity Risk, Compliance, and Threats)
- Optional KUs
    - Cyber Crime (Met by CYBXXX: Cyber Crime and adds new elective for current CJ students)
    - Fraud Prevention and Management (Met by AC313- Fraud Examination)

2. Reducing barrier to entry by utilizing existing classes and creating cyber pathways for current CMU students.

   Core:
    - CJ100- Introduction to Criminal Justice
    - CJ202- Criminal Law
    - CJ270- Criminal Procedure

   Electives:
    - AC313- Fraud Examination
    - Potentially several other opportunities to co-offer electives to cyber, CJ, accounting, etc. students

3. Offers CMU the opportunity to re-package this as an 18-credit hour cyber minor open to other majors.
    - CYB101: Intro to Cybersecurity
    - CYB205: Network Essentials
    - CYB310: Cybersecurity Law and Policy
    - CYB320: Cybersecurity Risk, Compliance, and Threats
    - CYB330: Cyber Security Operations
    - CYB340: Cyber Incident Response and Forensics

New Course Descriptions

1. **CYB101: Intro to Cybersecurity**
    - Pre-req: None
    - Designed for students with no security experience or background, this course will cover basic cybersecurity terminology and concepts. This course entirely covers the CompTIA Security+ common body of knowledge.

2. **CYB205: Network Essentials**
    - Pre-req: None
    - This course provides students with foundational networking knowledge needed to include network architecture, network operations, and network security. This course entirely covers the CompTIA Network+ common body of knowledge.
3. **CYB310: Cybersecurity Law and Policy**
    - Pre-req: Intro to Cybersecurity
    - This course examines legal and policy challenges stemming from rapidly evolving cybersecurity threats. Specific topics include intellectual property, jurisdictional considerations, international law, and cyber policy.
4. **CYB320: Cybersecurity Risk, Compliance, and Threats**
    - Pre-req: Intro to Cybersecurity
    - This course analyzes external and internal security threats, leading compliance frameworks (NIST, ISO, etc.), and risk management principles
5. **CYB330: Cyber Security Operations**
    - Pre-req: Network Essentials
    - This course uses cybersecurity principles to illustrate how they are applied to the modern enterprise. This course also introduces the concepts of red team/blue team and entirely covers the CompTIA PenTest+ common body of knowledge.
6. **CYB340: Cyber Incident Response and Forensics**
    - Pre-req: Cyber Security Operations
    - This course applies blue team tactics to the modern enterprise. This course also introduces the concepts of red team/blue team and entirely covers the CompTIA CySA+ common body of knowledge.
7. **CYB350: Cyber Crime**
    - Pre-req: Intro to Cybersecurity or CJ100- Introduction to Criminal Justice or other intro classes from other majors since this is an elective
    - This course explores how an interconnected world has modified how existing criminal activity is conducted and how new criminal opportunities have been created.

Central Methodist University
New Academic Program Proposal – Cybersecurity

Program Goals/Outcomes

Students with a Major in Cybersecurity will be able to recognize, discuss and explain information security principles and how those information principles apply to industry.

- Students will be able to demonstrate the information security risk analysis and describe/apply various information security tools.
- Students will be able to compare and contrast the domestic and international information security issues and legal issues.
- Students will develop technical and administrative skills and apply them to the information security industry.

Central Methodist Strategy

Develop a Cyber program that blends with an already strong Criminal Justice program that also meets NSA/DHS Center for Academic Excellence, Cyber Defense track, requirements.

Recommended CAE alignment (Cyber Defense Track):

Cyber Investigations

Knowledge Units (KU)s necessary to impart the necessary skills and abilities for performing technical analyses of computer incidents and intrusions to determine source, infiltration path, mechanism, system modifications and effects, damages, exfiltration path, data infiltrated, and residual effects.

To complete this specialization area, students must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- Technical Core KUs
    - Basic Networking
- Non-Technical Core KUs or Cyber Threats
    - Policy, Legal, Ethics, and Compliance
    - Security Risk Analysis
- Optional KUs
    - Cyber Crime

- Cybersecurity Ethics
- Forensic Accounting
- Fraud Prevention and Management
- IA Compliance
- Privacy

Draft BS Cyber Security Major Requirements (30 Hours)

<table>
<tr><th colspan="4">CMU Cyber Core (27 hours)</th></tr>
<tr><th>Course Name</th><th>Hours</th><th>Status</th><th>Alignment</th></tr>
<tr><td>CJ100- Introduction to Criminal Justice</td><td>3</td><td>Existing</td><td>CAE Support</td></tr>
<tr><td>CJ202- Criminal Law</td><td>3</td><td>Existing</td><td>CAE Support</td></tr>
<tr><td>CJ270- Criminal Procedure</td><td>3</td><td>Existing</td><td>CAE Support</td></tr>
<tr><td>CYB101: Intro to Cybersecurity</td><td>3</td><td>New</td><td>CompTIA Security+</td></tr>
<tr><td>CYB205: Network Essentials</td><td>3</td><td>New</td><td>Meets Req CAE KU
CompTIA Network+</td></tr>
<tr><td>CYB310: Cybersecurity Law and Policy</td><td>3</td><td>New</td><td>Meets Req CAE KU</td></tr>
<tr><td>CYB320: Cybersecurity Risk, Compliance, and Threats</td><td>3</td><td>New</td><td>Meets Req CAE KU</td></tr>
<tr><td>CYB330: Cyber Security Operations</td><td>3</td><td>New</td><td>CompTIA PenTest+</td></tr>
<tr><td>CYB340: Cyber Incident Response and Forensics</td><td>3</td><td>New</td><td>CompTIA CySA+</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><th colspan="4">CMU Cyber Electives</th></tr>
<tr><td>AC313- Fraud Examination</td><td>3</td><td>Existing</td><td>CAE Optional KU</td></tr>
<tr><td>CYB350: Cyber Crime</td><td>3</td><td>New</td><td>CAE Optional KU</td></tr>
</table>

Result

1. Alignment to apply for NSA/DHS Center for Academic Excellence, Cyber Defense
   - Technical Core KUs

    - Basic Networking (Met by CYBXXX: Network Essentials)
- Non-Technical Core KUs o Cyber Threats
    - Policy, Legal, Ethics, and Compliance (Met by CYBXXX: Cybersecurity Law and Policy)
    - Security Risk Analysis (Met by CYBXXX: Cybersecurity Risk, Compliance, and Threats)
- Optional KUs
    - Cyber Crime (Met by CYBXXX: Cyber Crime and adds new elective for current CJ students)
    - Fraud Prevention and Management (Met by AC313- Fraud Examination)

2. Reducing barrier to entry by utilizing existing classes and creating cyber pathways for current CMU students.

   Core:
    - CJ100- Introduction to Criminal Justice
    - CJ202- Criminal Law
    - CJ270- Criminal Procedure

   Electives:
    - AC313- Fraud Examination
    - Potentially several other opportunities to co-offer electives to cyber, CJ, accounting, etc. students

3. Offers CMU the opportunity to re-package this as an 18-credit hour cyber minor open to other majors.
    - CYB101: Intro to Cybersecurity
    - CYB205: Network Essentials
    - CYB310: Cybersecurity Law and Policy
    - CYB320: Cybersecurity Risk, Compliance, and Threats
    - CYB330: Cyber Security Operations
    - CYB340: Cyber Incident Response and Forensics

New Course Descriptions

1. **CYB101: Intro to Cybersecurity**
    - Pre-req: None
    - Designed for students with no security experience or background, this course will cover basic cybersecurity terminology and concepts. This course entirely covers the CompTIA Security+ common body of knowledge.

2. **CYB205: Network Essentials**
   - Pre-req: None
   - This course provides students with foundational networking knowledge needed to include network architecture, network operations, and network security. This course entirely covers the CompTIA Network+ common body of knowledge.
3. **CYB310: Cybersecurity Law and Policy**
   - Pre-req: Intro to Cybersecurity
   - This course examines legal and policy challenges stemming from rapidly evolving cybersecurity threats. Specific topics include intellectual property, jurisdictional considerations, international law, and cyber policy.
4. **CYB320: Cybersecurity Risk, Compliance, and Threats**
   - Pre-req: Intro to Cybersecurity
   - This course analyzes external and internal security threats, leading compliance frameworks (NIST, ISO, etc.), and risk management principles
5. **CYB330: Cyber Security Operations**
   - Pre-req: Network Essentials
   - This course uses cybersecurity principles to illustrate how they are applied to the modern enterprise. This course also introduces the concepts of red team/blue team and entirely covers the CompTIA PenTest+ common body of knowledge.
6. **CYB340: Cyber Incident Response and Forensics**
   - Pre-req: Cyber Security Operations
   - This course applies blue team tactics to the modern enterprise. This course also introduces the concepts of red team/blue team and entirely covers the CompTIA CySA+ common body of knowledge.
7. **CYB350: Cyber Crime**
   - Pre-req: Intro to Cybersecurity or CJ100- Introduction to Criminal Justice or other intro classes from other majors since this is an elective
   - This course explores how an interconnected world has modified how existing criminal activity is conducted and how new criminal opportunities have been created.