OLD DOMINION UNIVERSITY
PROPOSAL FOR A NEW MINOR, NEW INTERDISCIPLINARY MINOR
OR SIGNIFICANT CHANGES TO AN EXISTING MINOR

A minor may be chosen by students to support the major, to offer greater job opportunities to the student on graduation, or to provide recognition of study in a second academic area. Completion of an approved minor will meet the upper-division General Education requirement. A minimum of 12 credit hours, normally at the advanced level (300-400) in a specified field of study is required.

Interdisciplinary minors require 12 credit hours of 300/400-level courses selected from at least two different disciplines with a maximum of six credits from any one discipline. Three credit hours in the interdisciplinary minor may be in the major, if a major course is listed as an option for the interdisciplinary minor. As such, it will be credited toward both the major and the interdisciplinary minor.

Please refer to the Undergraduate Catalog for the complete policy on minors.

Minimum enrollment expectations for minors are five graduates in five years or the minor will be discontinued.

**Proposed Action (check one)**

- [ ] New Minor
- [x] New Interdisciplinary Minor
- [ ] Significant Changes to an Existing Minor

1. Name of proposed minor or minor to be changed:

Cybercrime

2. Description of proposed minor or change to an existing minor:

This interdisciplinary minor provides students with an understanding of the central concepts and issues in cybercrime. Students will be required to take the two introductory courses in the cybercrime and cybersecurity majors, respectively - CRJS 405 – Cybercrime, and CYSE 300 – Introduction to Cybersecurity. In these two core courses, students will learn the fundamental issues involved in cybersecurity (computer system architectures, critical infrastructures, cyber threats and vulnerabilities) and cybercrime (defining and describing the different types of computer-related crimes, the techniques used by law enforcement, and the legal issues inherent in combating cybercrime).

They can then expand their knowledge by taking electives in psychology, political science, criminal justice, information technology, or cybersecurity. This minor is differentiated from the cybersecurity minor in two ways: (1) the focus is on the criminal aspect of cyber - the theories of crime and deviance, criminal investigations, and law; (2) the focus is on social science and the human factors associated with cyber – as opposed to computer programming and networking.
3. Rationale for proposal:
   (address what the proposed minor will accomplish for students)

At the college level, liberal arts students need more options that increase their understanding of new technologies. We believe there is room for a minor that allows students to learn about the intersection of social issues and computer technology without requiring them to learn computer programming.

At the department level, a cybercrime minor may provide access to a new pool of students. The initial cohort of cybercrime majors were students who had an interest in computer technology, as it is *applied* to social issues, as opposed to computer programming or website design. Students across the university may also have this interest and as such will enroll in criminal justice courses. This can increase enrollment.

At the student level, the minor allows a student to broaden their skill set and increase their employability. The minor will allow a student who is focusing on social science to take technology courses, or a student majoring in a technology major to take courses in social science. An example would be an Information Technology major who has computer skills (e.g. basic programming or networking) and wishes to work for a federal agency. The student’s resume is strengthened by taking a course in Cyberlaw or White-Collar Crime. Similarly, the criminal justice major could benefit from taking courses in Introduction to Networking and Security or Digital Forensics.

4. Majors likely to enroll in the minor (for new minors):

With the rationales given above, these majors are likely to be interested:

- Criminal Justice
- Sociology
- Psychology
- Political Science
- Business
- Information Technology
- Cybersecurity

5. Projected enrollment and why (for new minors):

- In two years, the cybercrime major has grown to 68 majors. Given that a minor requires less investment, we can expect similar growth for the minor.

6. Proposed Effective Term:

- Fall 2019
7. Resources needed, including human resources, library resources, faculty resources, and funding resources:

- Cybercrime-specific courses, taught by faculty in criminal justice and sociology, will greatly enhance the program. These courses will expand the offerings within the cybercrime major, the criminal justice major, and the cybersecurity major. Faculty will be encouraged to create new courses. Dr. Caitlin Lynch is developing Youth, Crime, and Technology for this purpose.

8. Program requirements: [List below all courses required for the minor, the prerequisites, and the total hours required for the minor. Submit the appropriate information through the online Course Inventory Management (CIM) process in CourseLeaf (nextcatalog.odu.edu/courseadmin) for all new courses/course changes.]

The minor requires completion of 12 credit hours at the 300/400 level.

Prerequisites

- CRJS 215 – Introduction to Criminology*

Core (6 Hours):

- CRJS 405 – Cybercrime
- CYSE 300 – Introduction to Cybersecurity

Electives (6 Hours):

- CRJS 340 – White Collar Crime
- CRJS 344 – Social Science and Crime Mapping
- IT 315 – Introduction to Networking and Security
- IT 360T – Principles of Information Technology
- CRJS/CYSE 406 – Cyberlaw
- CYSE 407 - Digital Forensics
- PSYC 307 – Institutionalization of Human Centered Computing
- PSYC 344 - Human Factors
- POLS 350T – Technology and War
- CRJS (XXX)**

Notes

*Does not count towards major requirements
** A topics course approved by the program coordinator

1. With the approval of the program coordinator, courses that focus on cybersecurity can also fulfill the requirements of the minor.
2. Students must file a minor declaration form in 6000 Batten Arts & Letters.
9. Description (showing new copy or revised copy) for the next Undergraduate Catalog.
The interdisciplinary minor in cybercrime provides students with an understanding of crime and
deviance in the digital environment. Students will be required to take two introductory courses in the
cybercrime and cybersecurity majors, respectively. In these core courses, students will learn the
fundamental issues involved in cybersecurity (computer system architectures, critical infrastructures,
cyber threats and vulnerabilities) and cybercrime (defining and describing the different types of
computer-related crimes, the techniques used by law enforcement, and the legal issues inherent in
combating cybercrime). They can then expand their knowledge by taking electives in psychology,
political science, criminal justice, information technology, or cybersecurity. The minor aspires to
develop graduates who can think critically about how human behavior impacts and is impacted by
computer technologies.
Three credit hours in the interdisciplinary minor may be in the major if a major course is listed as an
option for the interdisciplinary minor. As such, it will be credited toward both the major and the
interdisciplinary minor. Interdisciplinary minors require 12 credit hours of 300/400-level courses
selected from at least two different disciplines with a maximum of six credits from any one discipline.
Course substitutions may be approved by the interdisciplinary minor coordinator.

10. Schedule for offering courses (include whether the minor can be completed in two years and
whether it will be available through Distance Learning) (for new minors):

The cybercrime, cybersecurity, and criminal justice majors are offered fully online. The minor
will be available for distance learning. However, some electives may not be available regularly
online (e.g. POLS 350T – Technology and War and CRJS 344 – Social Science and Crime
Mapping).

This minor can be completed in two years. A sample schedule is below:

**Fall 2019 – Student’s Junior Year**

Students complete one required course. These courses are offered at least once a year, and
usually both are offered every semester:
- CYSE 300 – Introduction to Cybersecurity *(or)*
- CRJS 405 – Cybercrime and Cybersecurity *(or)*

**Spring 2020 – Student’s Junior Year**
Students complete one required course. These courses are offered at least once a year, and
usually both are offered every semester:
- CYSE 300 – Introduction to Cybersecurity *(or)*
- CRJS 405 – Cybercrime and Cybersecurity *(or)*

**Fall 2020 – Student’s Senior Year**
One or two electives:
- A student majoring in information technology may choose:
  - CRJS 340 – White Collar Crime *(and/or)*
  - PSYC 344 - Human Factors
- A student majoring in criminal justice may choose:
- IT 315 – Introduction to Networking and Security (and/or)
- POLS 350T – Technology and War

**Spring 2021 – Student’s Senior Year**

*One or two electives:*

- A student majoring in information technology may choose:
  - CRJS/CYSE 406 – Cyberlaw (and/or)
  - CYSE 407 - Digital Forensics

- A student majoring in criminal justice may choose:
  - IT 360T – Principles of Information Technology (and/or)
  - PSYC 307 – Institutionalization of Human Centered Computing

**11. Effect on current department course schedule (for new minors):**

- Based upon the last two semesters, the courses listed above are currently being offered as a part of established majors regularly by full time faculty. There are no modifications needed.
APPROVED

Originator of Request  Roderick Graham  /2/19/2019

Signature

Date

College Dean  

Signature  /2/28/19

Date

Department Chair  Mona JE Danner  /2/19/2019

Signature  

Date

External Department (CYSE)  Hongyi Wu  /2/19/2019

Signature  

Date

External Department (PSYC)  Michelle L. Kelley  /2/19/19

Signature  

Date

External Department (IT)  Ling Li  /2/25/2019

Signature  

Date

Chair, Faculty Senate  

Signature  

Date

Chair, College Committee  

Signature  

Date

Provost  

Signature  

Date

ADMINISTRATIVE CODING

Effective Term  

Major Code  

College  

Degree Code  

Department  