MS in Cybersecurity, pre-2018 Curriculum

Core Courses (15 credits)
- INFO 517 – Principles of Cybersecurity
- INFO 679 – Information Ethics
- INFO 725 – Information Policy
- Math Requirement: CS 521 or ECES 521
- Networking Requirement: CS 544 or ECEC 631

Technical Electives (18 credits, choose 6 courses)
- CS 522: Data Structures and Algorithms II
- CS 543: Operating Systems
- CS 575: Software Design
- CS 576: Dependable Software Systems
- CS 590: Privacy
- CS 645: Network Security
- CST 604: Technology for Homeland Security
- CST 609: National Security Intelligence
- CST 614: Counterintelligence
- ECEC 621: High Performance Computer Architecture
- ECEC 622: Parallel Computer Architecture
- ECEC 623: Advanced Topics in Computer Architecture
- ECEC 632: Performance Analysis of Computer Networks
- ECEC 633: Advanced Topics in Computer Networking
- ECEC 641: Web Security I
- ECEC 642: Web Security II
- ECEC 643: Web Security III
- ECES 522: Random Processes & Spectral Analysis
- ECES 523: Detection & Estimation Theory
- ECES 621: Communications I
General Electives (12 credits)

The remaining courses needed to reach the minimum credit hour requirement for the degree program are considered general elective courses. General electives can be chosen from among the graduate course offerings of the College of Computing & Informatics; the Department of Electrical and Computer Engineering; and the Department of Mathematics. In order to have courses outside of these departments and schools count towards degree completion, they must be approved by the graduate advisors prior to registration for said courses.