A. Course Description

Credits: 4

Prerequisites: ICS 684 Cyberspace Security Engineering I

Lab Hours/ Weeks: Corequisites: None

Lecture Hours/ Week :

MnTC Goals: None

This course will be the second of a two-course series that introduces the interdisciplinary field of cyberspace security. The technical foundation for the cybersecurity defender is a particular combination of network, operating system, hardware (mobile, desktop, and server) and software engineering skills, all of which are required to protect and defend modern systems, networks and information assets. Students will explore in-depth technical foundations which underpin cybersecurity threats and corresponding defenses. Through hands-on training using Cyber Range students will gain necessary skills to begin supporting and implementing cyberspace security. This course will cover the following topics: Identity and Access Management (Physical and logical assets control, authentication, access control attacks, and access provisioning lifecycle), Security Assessment and Testing (Assessment and test strategies, security process data, and security control testing), Security Operations (Investigations, incident management, and disaster recovery, logging and monitoring, patch management and recovery strategies), and Software Development Security (understanding, applying, and enforcing software security, security in the software development lifecycle, and development environment security controls).

B. Course Effective Dates: 01/09/2017 - Present

C. Outline of Major Content Areas:

See Course Description for major content areas.

D. Learning Outcomes (General)

1. Manage identification, authentication, and authorization of people and devices and implement the related technologies
2. Use the principles of assurance and trust integrate assurance into software system requirements and designs.
3. Demonstrate expertise in reading peer-reviewed papers in cyberspace security, and explain them in writing.
4. Create and manipulate Access Control Matrices (ACMs), and use the theory of ACMs to demonstrate results related to the basic concepts
5. Design and validate security assessment and test strategies
6. Collect and analyze security process data and produce quality reports for different audiences.
7. Understand and apply foundational security operations concepts
8. Employ resources resource protection techniques and understand secure provisioning of these resources.
9. Conduct incident management, logging, and monitoring activities.
10. Understand requirements for investigation types and support investigations.
11. Understand and apply security in the software development life cycle and enforce security controls in development environment

E. Learning Outcomes (MN Transfer Curriculum)

This contains no goal areas.

G. Special Information