CYPD 631. Cybersecurity Compliance Methodologies Lab I. 3 credits

Credits: 3
Classroom: Online
Class Hours: Weekly online engagement, 20 hours; biweekly virtual seminars alternate Saturdays 10AM–12:00 PM, ET
Office Hours: Virtual, by appointment
Instructor: TBD
Phone: TBD
Email: TBD
Prerequisites: CYSE 630 or equivalent, or permission of the instructor
Text: Mastering the Risk Management Framework Revision 2 by James Broad
Materials: NIST SP 800-53, NIST SP 800-171 and FedRamp documentation

Course Description and Objectives:
In a virtual lab system, students execute the NIST RMF Steps 1-3: Categorization, Security Control Selection and Security Control Assessment, and complete the associated analysis and documentation as required by NIST/FedRAMP/CMMC.

Assessment Objectives:
- Demonstrate the ability to apply risk management compliance methods to categorize the risk exposure of a system
- Demonstrate the ability to identify the controls required to achieve the system risk categorization
- Demonstrate the ability to conduct privacy analysis and produce a privacy assessment
- Demonstrate the ability to develop an Information Systems Continuous Monitoring (ISCM) strategy

Course Outline:
The following is a tentative list of course projects which will enable students to demonstrate the ability to apply the NIST RMF Steps 1-3, in order to:

1. Produce an updated SSP
2. Integrate a FedRAMP SSP
3. Complete a FIPS 199 System Categorization
4. Produce a NIST Security Control Selection
5. Produce a PTA worksheet/template
6. Produce PIA worksheet/template
7. Remediate or write CMMC accreditable security controls
Grading
The grading will be based on course engagement, assignments, and projects. The final grade will be determined by weighing each component as follows:

- Asynchronous engagement: 40%
- Virtual seminar engagement: 12%
- Assignments: 24%
- Projects: 24%