CYBERSECURITY (CYB)

CYB 110 Cybersecurity and Privacy (3 credits)
An introductory survey of the issues and complexity of cybersecurity and privacy in the digital age. Cybersecurity and privacy foundational concepts, case studies of cybersecurity breaches, application of cybersecurity for business, and social media and the general populace. Survey of common threats, threat actors, and responses. Survey of applicable laws.

CYB 210 Cybersecurity Architectures and Management (3 credits)
Introduces the components in an information technology system and their roles in system operation. Teaches students how to use these components to develop plans and processes for a holistic approach to cybersecurity for an organization.
Prereqs: CYB 110

CYB 220 Secure Coding and Analysis (3 credits)
Describes the characteristics of secure programs and the ability to implement programs that are free from vulnerabilities. Practice evaluating software, including adding security mechanisms into software and testing software for vulnerabilities. Two lectures and one 2-hour lab per week.
Prereqs: CS 121

CYB 310 Cybersecurity Technical Foundations (3 credits)
Provides students with basic information about the various threats that may be present in the cyber realm and introduces architectural mitigation strategies including cryptography.
Prereqs: CYB 110, CS 240

CYB 330 Networking Fundamentals (3 credits)
Covers common network protocols, how network components interact, and how networks evolve over time. Students expand their familiarity with network vulnerabilities. Typically Offered: Fall.
Prereqs: CYB 210, CS 240

CYB 340 Network Defense (3 credits)
Covers concepts used in defending a network and the basic tools and techniques that can be taken to protect a network and communication assets from cyber threats. Provides students with knowledge and skills related to detecting and analyzing vulnerabilities and threats and taking steps to mitigate associated risks.
Prereqs: CYB 310, CYB 330

CYB 350 Operating System Defense (3 credits)
This course provides fundamentals of secure operating system administration and hardening. Provides students with an understanding of the authorities, roles, and steps associated with cyber operations.
Prereqs: CYB 310

CYB 380 Cybersecurity Lab I (3 credits)
This hands-on laboratory class allows students to get practical experience related to the cybersecurity threats, mitigations, and scenarios they have been introduced to in other courses. This includes classic buffer overflow and SQL injection style vulnerabilities, network monitoring, as well as Windows and Linux security configurations. 6 hours of lab per week.
Prereqs: CS 240
Coreqs: CYB 310, CYB 330

CYB 381 Cybersecurity Lab II (3 credits)
This hands-on laboratory class allows students to get practical experience related to cybersecurity threats, mitigations, and scenarios they have been introduced to in other courses. This course builds on CYB 380 by focusing on more advanced threats and mitigations. 6 hours of lab per week.
Prereqs: CYB 310, CYB 380
Coreqs: CYB 340, CYB 350

CYB 400 Seminar (1-16 credits)

CYB 401 Cybersecurity as a Profession (1 credit)
1 credit Ethical, legal, social, and intellectual property issues; current research topics; and other issues of importance to the professional cybersecurity researcher. Graded P/F. Graded Pass/Fail.
Prereqs: Senior Standing in Cybersecurity

CYB 404 (s) Special Topics (1-4 credits, max arranged)
Joint-listed with CYB 504
Special topic courses in the subject are often offered to allow students to learn topics of current interest that are not covered in permanent courses in the corresponding subject. Special topic courses cover topics and have learning outcomes and required academic activities and deliverables that are specific to each course offering. Cybersecurity (CYB) special topic courses at the undergraduate level may be chosen as electives toward a Bachelor of Science (BS) in Cybersecurity (CYB), Computer Science (CYB), or Computer Engineering (CE) degree. For students in all colleges, some special topic courses may be used to complement a student's interdisciplinary degree plan. Cybersecurity (CYB) special topic courses at the graduate level are usually used to complement the graduate study plan for students pursuing a Master's (MS) or Doctoral degree (PhD) in Cybersecurity (CYB) or Computer Science (CS). They may also be used to complement graduate study plans for students in the College of Engineering or graduate students in other colleges pursuing a multidisciplinary graduate degree. Significant additional work and performance required for graduate-level credit.
Prereqs: Junior standing or graduate standing or instructor permission

CYB 420 Digital Forensics (3 credits)
Cross-listed with CS 447
Joint-listed with CS 547, CYB 520
This course covers modern procedures, techniques, and best practices for digital forensic data acquisition, analysis, and case building. Covered topics and knowledge areas include (a) Applicable laws, policies, rules, procedures and best practices, and selected digital forensics techniques and tools (DFS); (b) Processes, techniques, tools, and best practices for static digital forensic data acquisition, analysis, and reporting from different host systems (HOF) and raw media (MEF). At the end of this course, students should have the knowledge, skills, and abilities to be able to appropriately prepare, perform, and record digital forensic investigation tasks on a selected set of media and hosts, of varied types. This including knowledge, skills, and abilities to: (1) Identify and describe applicable laws, policies, procedures, and static acquisition and analysis techniques and best practices for digital forensic investigations; (2) Identify the appropriate tools for a given forensic task on a given type of media, host, or image; and (3) Select and successfully use a variety of digital forensic tools for acquiring, analyzing, and recording case information. Hands-on and/or laboratory work is an essential component in this course. Significant additional work and performance required for graduate-level credit. Typically Offered: Fall.
Prereqs: CYB 310

CYB 440 Software Vulnerability Analysis (3 credits)
Provide students with a thorough understanding of system vulnerabilities, to include what they are, how they can be found/identified, the different types of vulnerabilities, how to determine the root cause of a vulnerability, and how to mitigate their effect on an operational system. Provide students with the ability to describe why software assurance is important to the development of secure systems and describe the methods and techniques that lead to secure software.
Prereqs: CYB 220, CYB 310

CYB 480 Cybersecurity Senior Capstone Design I (3 credits)
Capstone design sequence for cybersecurity science majors. Formal development techniques applied to definition, design, coding, testing, and documentation of a comprehensive cybersecurity. Projects are customer-specified, include real-world design constraints, and usually encompass two semesters. Students work in teams. Significant lab work required.
Prereqs: CS 383, CYB 381, ENGL 317, Senior Standing

CYB 481 Cybersecurity Senior Capstone Design II (3 credits)
General Education: Senior Experience
Continuation of CYB 480. Application of formal design techniques to development of a large cybersecurity science project performed by students working in teams. Significant lab work required. Typically Offered: Fall and Spring.
Prereqs: CS 383, CYB 381, CYB 480, ENGL 317

CYB 498 (s) Cybersecurity Internship (1-3 credits)
This course may be used to gain academic credit for knowledge, skills, and abilities acquired, enhanced, or refined through internal or external internships. Internship objectives and expected outcomes under this subject must be related to the subject area. Internships must include the following documents and/or deliverables: (a) internship proposal and plan including objectives, weekly hours, summary of planned tasks, or an external employer offer letter, plus a short description of how the internship supports the students' academic and career goals; (b) status update meetings and progress reports; (c) preparation and writing of an end of internship deliverable; and (d) enrollment in the University of Idaho's Internship Practicum Liability (details of this may be found on the UI Risk Management website). Examples of possible end of internship deliverables are: (1) an internship objectives' achievement assessment and lessons learned report and/or presentation, (2) an academic manuscript or portion thereof, (3) well-documented source code. The frequency and format of the intermediate and/or final deliverables must be agreed upon between the student and the internship advisor and/or coordinator before the internship begins. Objectives and learning outcomes will be assessed using a qualitative assessment method based on the quality and timeliness of the agreed upon deliverables. All internships, whether external or internal and paid or unpaid, require the approval of the student's advisor, the corresponding internship coordinator, and the University of Idaho's Risk Management office before internship start. Off-campus internships for international students also require the prior approval of the University of Idaho's International Programs Office (UI-IPO) and must be related to the student's area of study and support a student's academic and career objectives and pursued degree(s).
Prereqs: Instructor permission

CYB 499 (s) Directed Study (1-4 credits, max arranged)
Directed study courses in the subject are offered to allow students to earn academic credit for independent but guided study. Directed study courses are often offered to support students in the acquisition of prerequisite knowledge and skills or in the acquisition of knowledge and skills not usually covered by permanent courses. Directed study courses have course objectives, topics, learning outcomes, and required academic activities and deliverables that are specific to each course and section offering.
Prereqs: Instructor permission

CYB 500 (s) Master's Research & Thesis (1-10 credits)
This course allows graduate students to earn academic credit for performing research, design, development, verification and validation, documentation, writing, and academic communication activities toward the thesis degree requirement when pursuing a Master of Science (MS) in Cybersecurity (CYB) degree with thesis option. A maximum of ten (10) credits of Master's Research and Thesis may be used toward a Master's degree graduate study plan. A minimum grade of B is required for all credits within a graduate study plan. Students must be registered for a minimum of one (1) credit in each and all terms in which they are performing graduate research and thesis activities.

CYB 501 (s) Cybersecurity Graduate Seminar (1-3 credits, max 6)
This course enables colleges and departments to offer seminar-style courses in any given term and at the graduate level. Seminar-style courses in the subject are offered to allow students to learn about and discuss topics of importance to the pursued degree. Different seminar courses cover topics and have learning outcomes and required academic activities that are specific to each course offering. Examples of topics covered and discussed in seminar-style courses are: current research, discipline's best practices, history and future of the discipline, professional practice, professional communication, ethical issues, and technological and societal implications of the discipline and its practice. Graduate-level seminar-style course offerings usually require students to read, prepare, discuss, lead, and present, orally and/or in writing on the course offering topics. Typically Offered: Fall and Spring.
Prereqs: Graduate standing

CYB 502 (s) Graduate Directed Study (1-4 credits, max arranged)
Graduate-level directed study courses in the subject are offered to allow students to earn academic credit for independent but guided study. Graduate-level directed study courses are often offered to support students in: (a) the acquisition of needed prerequisite knowledge and skills, (b) the acquisition of knowledge and skills not usually covered by permanent courses, or (c) the conduct of research not directly related to a graduate project, thesis, or dissertation. Directed study courses have course objectives, topics, learning outcomes, and required academic activities and deliverables that are specific to each course and section offering.
Prereqs: Instructor permission

CYB 504 (s) Special Topics (1-4 credits, max arranged)
Joint-listed with CYB 404
Special topic courses in the subject are often offered to allow students to learn topics of current interest that are not covered in permanent courses in the corresponding subject. Special topic courses cover topics and have learning outcomes and required academic activities and deliverables that are specific to each course offering. Cybersecurity (CYB) special topic courses at the undergraduate level may be chosen as electives toward a Bachelor of Science (BS) in Cybersecurity (CYB), Computer Science (CYB), or Computer Engineering (CE) degree. For students in all colleges, some special topic courses may be used to complement a student's interdisciplinary degree plan. Cybersecurity (CYB) special topic courses at the graduate level are usually used to complement the graduate study plan for students pursuing a Master's (MS) or Doctoral degree (PhD) in Cybersecurity (CYB) or Computer Science (CS). They may also be used to complement graduate study plans for students in the College of Engineering or graduate students in other colleges pursuing a multidisciplinary graduate degree. Significant additional work and performance required for graduate-level credit.
Prereqs: Junior standing or graduate standing or instructor permission

CYB 507 CS and Cyber Research Methods (3 credits)
Cross-listed with CS 507
This course introduces graduate students to approaches, methods, techniques, tools, and legal and ethical rules and regulations for planning, designing, performing, evaluating, and reporting computer science and cybersecurity research and results. In this course, students should gain the needed knowledge and skills to be able to: (1) Identify appropriate publication venues and adequately perform related literature searches; (2) Critically read and interpret related research questions, methods, experiments, and results; (3) Develop a scientific research question; (4) Develop a research plan with corresponding research hypothesis and hypothesis testing experiments; (5) Analyze research experiment results; (6) Present research and results to a variety of audiences in written and oral form; (7) Identify applicable laws, such as human subjects research and conflicts of interest regulations, and ethical and non-ethical behaviors in the conduct of research.
Prereqs: Graduate standing or instructor permission

CYB 520 Digital Forensics (3 credits)
Cross-listed with CS 547
Joint-listed with CS 447, CYB 420
This course covers modern procedures, techniques, and best practices for digital forensic data acquisition, analysis, and case building. Covered topics and knowledge areas include (a) Applicable laws, policies, rules, procedures and best practices, and selected digital forensics techniques and tools (DFS); (b) Processes, techniques, tools, and best practices for static digital forensic data acquisition, analysis, and reporting from different host systems (HOF) and raw media (MEF). At the end of this course, students should have the knowledge, skills, and abilities to be able to appropriately prepare, perform, and record digital forensic investigation tasks on a selected set of media and hosts, of varied types. This including knowledge, skills, and abilities to: (1) Identify and describe applicable laws, policies, procedures, and static acquisition and analysis techniques and best practices for digital forensic investigations; (2) Identify the appropriate tools for a given forensic task on a given type of media, host, or image; and (3) Select and successfully use a variety of digital forensic tools for acquiring, analyzing, and recording case information. Hands-on and/or laboratory work is an essential component in this course. Significant additional work and performance required for graduate-level credit. Typically Offered: Fall.

CYB 536 Advanced Information Assurance Concepts (3 credits)
Cross-listed with CS 536
This course covers theory, approaches, techniques, and best practices for (a) Secure and resilient system and network architectures (IAA); (b) Cybersecurity compliance (IAC); (c) Cybersecurity standards (IAS); and (d) Security risk analysis (SRA). At the end of this course, given examples of cyber system models and scenarios, architectures, and implementations of different types and of varied complexity, students should have the knowledge, skills, and abilities to be able to: (1) Understand organizational and/or cyber-system requirements, architecture, design, and implementation; (2) Describe and analyze the system with appropriate detail; (3) Develop a threat model; (4) Identify potential vulnerabilities; (5) Identify appropriate risk analysis processes and standards; (6) Perform risk analysis and assessment; (7) Identify, evaluate, design, apply, and document security and resiliency enhancements and risk removal or mitigation approaches, tasks, and security controls. Such approaches, tasks, and controls including a combination of the following types: organizational, policy, technical, human factors, processes, protocols, techniques, and documents as appropriate.
Prereqs: Graduate standing and instructor permission

CYB 540 Advanced Networking & Security (3 credits)
This course covers the following topics and knowledge areas: (a) Advanced networking technology, algorithms, and protocols, and their cybersecurity implications (ANT) and (b) Wireless and mobile device algorithms, technologies, and protocols, and their cybersecurity implications (MOT). At the end of this course, students should have the knowledge, skills, and abilities to be able to: (1) Identify, classify, and describe, with detail, key modern networking and security algorithms, technologies, and protocols at and across several layers of the networking stack and for wired and wireless media; (2) Identify, classify, and describe advanced approaches, technologies, and protocols for secure and private digital networking within an enterprise and across federated domains, this including the IT, IoT, and mobile device realms. Several advanced and/or state-of-the-art networking and security technologies, algorithms, and protocols will be investigated in great depth and include lab-based hands-on implementations, investigations, and/or experiments. Typically Offered: Fall.
Prereqs: Graduate standing and Instructor permission

CYB 599 (s) Non-thesis Master's Resrch (1-6 credits, max 30)
This course allows graduate students to earn academic credit for performing research, design, development, verification and validation, documentation, writing, and academic communication activities toward the non-thesis research or graduate project degree requirement when pursuing a Master of Science (MS) in Cybersecurity (CYB) degree with non-thesis option. A maximum of six (6) credits of CYB 599 may be used toward a Master's degree study plan. A minimum grade of B is required for all credits within a graduate study plan. Students must be registered for a minimum of one (1) credit in each and all terms in which they are performing non-thesis graduate research or project activities. Typically Offered: Fall and Spring.
Prereqs: Graduate standing and Instructor permission

CYB 600 Doctoral Research and Dissertation (1-45 credits)
Credit arranged Typically Offered: Varies.
Coreqs: PhD Standing in the Cybersecurity PhD program