ABET
Self-Study Report

for the

Cyber Operations Program

at

United States Naval Academy

Annapolis, MD

June 30, 2017

CONFIDENTIAL

The information supplied in this Self-Study Report is for the confidential use of ABET and its authorized agents, and will not be disclosed without authorization of the institution concerned, except for summary data not identifiable to a specific institution.

Program Self-Study Report
for
CAC of ABET Reaccreditation

BACKGROUND INFORMATION

A. Contact Information

List name, mailing address, telephone number, fax number, and e-mail address for the primary pre-visit contact person for the program.

Dr. Allen Parrish, Chair
101 Leahy Hall
Cyber Science Department
117 Decatur (17-B)
United States Naval Academy
Annapolis, MD 21402
Phone: 410-293-0953
Email: aparrish@usna.edu

B. Program History

Include the year implemented and the date of the last general review. Summarize major program changes with an emphasis on changes occurring since the last general review.

The Cyber Operations (SCY) Program was implemented in the fall of 2013. The SCY Program underwent an ABET review during the 2016-17 cycle under the CAC General Criteria only (no applicable program criteria existed at the time of the review). There were no shortcomings identified from the visit, so we anticipate an NGR accreditation action in July 2017 from that process.

This review is for the purpose of evaluating the program under the Program Criteria for Cybersecurity programs. While the review is not required to maintain our accreditation under the General Criteria, we volunteered to participate in order to provide assistance to ABET and the profession in evaluating the new Program Criteria on a pilot basis. No significant changes to the curriculum have been made since our general review in the 2016-17 cycle[1], although we have made some changes to the assessment process.

With regard to the overall history of the program, the United States Naval Academy (USNA) is charged with ensuring that all *midshipmen* (undergraduate students at USNA) receive an education that is sufficient to prepare them to preserve, protect, and defend the nation. Influenced by President Obama's May 2009 Cyberspace Policy Review, which included the need to "expand and train the workforce, including … cyber security

[1] We did make a minor change to the curriculum this past spring semester. For Class of 2020 and later, we replaced SM286 (Discrete Math and Probability – a 3-hour course) with SM242 (Discrete Math and Probability – a 4-hour course). The addition of one mathematics hour required that we drop ES360 (a one-hour general education course on embedded systems, which is subsumed by a course in the major that was already required – SY202).

expertise in the Federal government"[2], a committee of USNA faculty members was charged with exploring and defining the scope of understanding of cyber security needed by midshipmen in their capacity as future naval officers. The committee worked with the Office of the Chief of Naval Operations and Commandant of the Marine Corps staffs, analyzed the other service academies' inclusion of cyber warfare concepts in their curricula, and examined various other academic cyber security programs.

In August 2009, USNA's Cyber[3] Warfare Ad Hoc Committee delivered its Initial Report that included a recommendation to create a required core course providing a technical foundation for undergraduate cyber warfare education for all students, regardless of academic major. The unanimous view of the committee was that the course be technically oriented, focused on naval applications and case studies, and delivered in a hands-on, lab-based format. This course was intended to form the technical basis for continued cyber security education that could be expanded upon as appropriate within the various majors.

In April 2010, USNA's Academic Dean & Provost formed a second committee, the Ad Hoc Committee on Cyber Security Curriculum Options, charged with examining a variety of approaches for integrating cyber concepts into the core curriculum. That committee ultimately recommended a two-course, technically-oriented sequence: the first course to be taken by all students during their initial year, and the second to be taken by all students during their third year. The first course, SY110 – Fundamentals of Cyber Security, was rolled out successfully and on schedule with the first offering in Fall of Academic Year (AY) 2012[4]. The second course, EC310 – Cyber Security II, was rolled out in the Fall of AY 2014 (i.e., Fall of 2013).

After deploying these two core courses, resources became available to develop the new Cyber Operations major that we are proposing here for ABET accreditation. Given the interdisciplinary elements of the new major and the time and resources required to establish a new academic department, the most effective mechanism for startup and rapid deployment of the major was to establish an interdisciplinary center known as the *Center for Cyber Security Studies (CCSS)*. The CCSS was utilized to organize the program and determine the most rapid path to effective deployment in order to meet the critical needs of the Navy – this included the design of new courses as well as the identification of appropriate existing courses to be utilized within the major. Faculty were initially identified either from existing programs, or were hired within the CCSS. The major was first advertised to freshmen (rising sophomores) during Spring AY2013; the major officially came on-line the following semester (Fall AY2014).

---

[2] President's Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, May 2009. DOI=http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[3] Note that this self-study frequently uses the term "cyber" both by itself, and in conjunction with other words (e.g., cyber security, cyber warfare, cyber defense, etc.). We take "cyber" to generally mean a digitally centric ecosystem of software, hardware, networks and peripheral devices that is at risk of crime, terrorism, espionage and warfare. Such "cyber" ecosystems are heavily digital, although not exclusively – almost all digital systems subsume analog components, especially at the system boundaries. It should be noted that cyber is not a well-defined concept, and may be interpreted in multiple ways within the literature. Our notion of cyber relies heavily on computing as the root discipline from which its technical content is derived.

[4] It is common at the Naval Academy to refer to academic years (Fall-Spring) by the year of the Spring semester. That is, AY 2012 consists of the Fall semester in calendar year 2011 and Spring semester in calendar year 2012. However, rather than referring to that Fall semester as "Fall 2011" (typical of many institutions), it is normally referred to as "Fall of (Academic Year) 2012." In this report, we will refer to semesters in terms of the *academic* year to which they belong, e.g., Fall AY2016 means Fall of the *calendar* year 2015.

While the CCSS provided the fastest path to initial deployment, it lacked the standing of an academic department to most effectively institutionalize the Cyber Operations Program. In the Fall AY2016 (i.e., August 2015), a new Cyber Science Department was formed, leaving the CCSS as a support unit and to provide leadership in the promotion of cyber-related activities and programs across the institution and beyond. Many faculty members who were formally housed in the CCSS moved over into Cyber Science Department or were given joint appointments in both entities. Most of the faculty members working in the department are housed in Leahy Hall. Approval has also been granted to build a new Cyber Science building on the yard, which is expected to come on-line at the beginning of Fall AY2020.

Thus, the program has gone through rapid growth and evolution and has settled on a structure with a Department "owner" (Cyber Science), supported heavily in terms of technical courses by three other academic departments (Computer Science, Electrical and Computer Engineering, and Systems Engineering) – with the CCSS supporting the *program* (not just the Cyber Science *Department*) by providing resources, external collaborators and coordination among the various stakeholders. The first graduating class of 27 midshipmen completed their course of study in Spring AY2016, while the second graduating class of 45 midshipmen completed their course of study in Spring AY2017. There are currently 143 midshipmen SCY majors from the rising senior, junior and sophomore classes. Freshmen do not declare a major until the spring semester of their freshman year.

C. Options

List and describe any options, tracks, concentrations, etc. included in the program.

There are no options, tracks, or concentrations in the program.

D. Program Delivery Modes

Describe the delivery modes used by this program, e.g., days, evenings, weekends, cooperative education, traditional lecture/laboratory, off-campus, distance education, web-based, etc.

The program is a traditional four-year, day-time resident program involving lectures and labs. The Naval Academy operates on a semester schedule, graduating midshipmen in May. Class and laboratory sessions for the program are offered between the hours of 7:55 am and 3:30 pm, Monday through Friday. Examinations common to large-enrollment classes, called X-period exams, can extend the regular-class hours from 6:55 am. These exams are scheduled twice a semester at the six- and twelve-week points. The program is not delivered in the evenings or weekends; there is no off-campus work and no distance education.

E. Program Locations

Include all locations where the program or a portion of the program is regularly offered (this would also include dual degrees, international partnerships, etc.).

All classes are delivered on site in Annapolis, Maryland. There are opportunities for midshipmen to participate in exchange programs at the other service academies and semester study abroad with foreign universities. These exchange opportunities are handled on an individual basis. In such cases the midshipmen work with their advisors to ensure that progress towards graduation is maintained.

F. Public Disclosure

Provide information concerning all the places where the Program Education Objectives (PEOs), Student Outcomes (SOs), annual student enrollment and graduation data is posted or made accessible to the public. If this information is posted to the Web, please provide the URLs.

This information is posted on the Cyber Science Department website. The Program Educational Objectives can be found at http://www.usna.edu/CyberCenter/Academics/peo.php, and the Student Outcomes can be found at http://www.usna.edu/CyberCenter/Academics/so.php. The annual student enrollment and graduation numbers are available at: http://www.usna.edu/CyberDept/Assessment/EnrollmentGraduationRates.php. These URLs are available on the Internet for access by the general public.

G. Deficiencies, Weaknesses or Concerns from Previous Evaluation(s) and the Actions Taken to Address Them

Summarize the Deficiencies, Weaknesses, or Concerns remaining from the most recent ABET Final Statement. Describe the actions taken to address them, including effective dates of actions, if applicable. If this is an initial accreditation, it should be so indicated.

The Draft Statement from our 2016-17 visit revealed no shortcomings. We do not anticipate any changes to the Final Statement.

GENERAL CRITERIA

CRITERION 1. STUDENTS

For the sections below, attach any written policies that apply.

A. Student Admissions

Summarize the requirements and process for accepting new students into the program.

Students are admitted to the Naval Academy with no restriction as to major. The Academy has a Chief of Naval Operations (CNO) mandate of having a minimum of 65% of those commissioned into the US Navy having completed a technical Science, Technology, Engineering, or Mathematics (STEM) degree. This goal is considered in evaluating applicants for admission. The admissions criteria for entrance to the Naval Academy apply to all candidates. Candidates must qualify medically and scholastically, and pass a physical aptitude test. To receive an offer of appointment to the Naval Academy, an applicant must also obtain a nomination from an official source. There are many nomination sources including US Representatives, US Senators, and the Vice President of the US. Applicants must be US citizens of good moral character, must be at least 17 years old and not past their 23rd birthday on July 1st of the year they enter. Applicants must be unmarried, not pregnant, and have no dependents.

As a recent sample, for the Class of 2019, there were 1,373 applicants offered admission out of 16,101 applications. From the 1,373 who were offered admission, 1,191 enrolled. Of these students, 92% were varsity athletes in high school, 66% were National Honor Society members, and 88% were active in community service. The middle 50% of the entering class achieved SAT verbal scores in the 570 to 690 range and SAT math scores in the 620 to 690 range. Midshipmen were admitted from every state in the Nation, as well as Guam, Puerto Rico, and the U.S. Virgin Islands. The Class of 2019 also includes 12 international students from: Albania (1), Cambodia (1), Georgia (1), Korea (1), Malaysia (1), Montenegro (1), Philippines (2), Taiwan (1), Thailand (1) and Turkey (2). The Naval Academy strives to recruit and admit a diverse student population. The Class of 2019 includes 12% midshipmen of Hispanic background, 10.57% of African American background, and 14.36% of Asian American background.

The first ever class of Cyber Operations majors who started the program in Fall AY2014 was restricted to a size of 40; 36 students actually enrolled. We limited the size of the first class to make sure that the required teaching resources for the major would be available. Subsequent classes have not had limits placed on size. More recently (for the Class of 2020 – last year's freshmen), 72 students enrolled in the major.

B. Evaluating Student Performance

Summarize the process by which student performance is evaluated and student progress is monitored. Include information on how the program ensures and documents that students are meeting prerequisites and how it handles the situation when a prerequisite has not been met.

The first academic evaluation in a midshipman's Academy experience occurs during Plebe Summer, which is the summer preceding the fourth class (freshman or Plebe) year. During Plebe Summer, all entering midshipmen have the option of taking placement exams in English, mathematics, and science. Midshipmen (abbreviated as "MIDN") may elect to take placement exams in other discipline-specific areas such as Economics, History, Political Science, and foreign languages.

Evaluation of progress in courses is through a traditional A–F grading system, where A denotes excellent performance, B denotes above average performance, C denotes average or satisfactory performance, D denotes marginal but satisfactory performance, and F denotes failure. Each instructor is responsible for entering letter grades (A, B, C, D, or F) at 6-, 12-, and 16-week interim-marking periods, and at the end of each course. In courses where a final exam is given, which are nearly all courses, the final exam grade is also recorded. An example of an end-of-semester grade report is shown in Table 1-1.

Table 1-1. Example Grade Report after Conclusion of a Semester

Ac Yr	Sem	Course	Title	Section	6-Week	12-Week	End of Term	Final Exam	Course
2016	SPRING	SY202	CYBER FUNDAMENTALS II	4001	B	A	A	A	A
2016	SPRING	SY304	SYSTEMS PROGRAMMING/OS FUNDAMENTALS	3002	A	B	B	A	A
2016	SPRING	SM230	PROBABILITY WITH NAVAL APPLICATIONS	2001	A	A	A	A	A
2016	SPRING	HH216	THE WEST IN THE MODERN WORLD	2006	A	B	A	B	A
2016	SPRING	NN210	BASIC NAVIGATION	5001	A	A	A	A	A
2016	SPRING	SP212	GEN PHYSICS II	1123	B	C	C	D	C

Course grades are weighted based on credits to arrive at the student's *Quality Point Rating (QPR)* for that semester. The QPR is equivalent to the GPA commonly used in civilian universities. The numeric grade is based on a 4-point grading system: A = 4.0, B = 3.0, C = 2.0, D = 1.0, and F = 0.0. Like GPAs, QPRs are computed and stated on a per semester basis, or alternatively, QPRs may be computed in a cumulative fashion and are thus known as "Cumulative QPRs."

A database application known as the *Midshipman Information Database System (MIDS)* is used to calculate semester QPRs and maintain cumulative QPRs in the major and overall. A sample academic history after seven semesters is shown in Table 1-2. The QPR does not include grades for professional drills, conduct, military performance, or physical education; a separate "military QPR" is computed just for those items. All midshipmen must maintain a minimum cumulative QPR of 2.0 after completing their course of study for graduation and commissioning.

Table 1-2. Illustrative Academic History for a midshipman from MIDS

Ac Yr	Sem	Sem Hrs	Cum Hrs	Cum Maj Hrs	Sem Qual Pts	Cum Qual Pts	Cum Maj Qual Pts	Sem QPR	Cum QPR	Cum Maj QPR	Sem Mil QPR	Cum Mil QPR
2016	Fall											
2015	Spring	22	116	36	85	444	131	3.86	3.83	3.64	3.64	3.7
2015	Fall	19	94	23	65	359	82	3.42	3.82	3.57	3.87	3.71
2014	Spring	22	75	13	82	294	49	3.73	3.92	3.77	3.62	3.67
2014	Fall	19	53	6	76	212	24	4	4	4	3.83	3.69
2013	Spring	18	34	0	72	136	0	4	4	0	3.5	3.63
2013	Fall	16	16	0	64	64	0	4	4	0	3.81	3.81

Grades received in military performance and professional courses are used to compute a midshipman's rank in class called the *Order of Merit (OOM)*. The OOM is used to assist in determining the service assignment of each midshipman. Approximately 75% of MIDN are commissioned in the Navy and 25% are commissioned in the Marine Corps. Per OPNAVINST 5450.330, USNA must commission no less than 95% of those midshipmen (MIDN) being appointed in the Navy as unrestricted line officers (surface, aviation, submarine, special warfare, and explosive ordinance disposal.) The remaining 5% are commissioned in restricted line or staff communities. The OOM is a weighted representation of grades received in academics, military performance, conduct, physical education, athletics, and professional competence. Academic performance accounts for 65% of the OOM.

C. Transfer Students and Transfer Courses

Summarize the requirements and process for accepting transfer students and transfer credit. Include any state-mandated articulation requirements that impact the program.

The Naval Academy is a four-year academic and military training program that requires participation for the entire four-year period. The Naval Academy does not allow students to transfer into the program; all students must start out as fourth class midshipmen (freshman) and must go through the Plebe Summer program. Please see section E on *Work in Lieu of Courses* for information regarding "validating" courses based on previous work in high school or at another institution of higher learning. Regardless of validated

courses, however, all students remain in the program for exactly four years in order to complete their required military training and graduate with their entering cohort group (e.g., freshmen (plebes) entering during Fall AY2017 are part of the "Class of 2020," and will graduate and be commissioned as Navy officers as a group in May 2020).

D. Advising and Career Guidance

Summarize the process for advising and providing career guidance to students. Include information on how often students are advised, who provides the advising (program faculty, departmental, college or university advisor).

The structure for all academic programs at the Naval Academy consists of a freshman, or Plebe, year component and an upper class, or majors, component. The Plebe-year curriculum is common to all midshipmen. Academic advising is coordinated by the Deputy Director of Academic Advising, Dr. Mike Williams.

Faculty and staff volunteer as Plebe advisors, many of whom have served in their capacities for five or more years. Each Company[5] has a Plebe-advising team that typically has three advisors. For each Plebe-advising team a person who has served for multiple years as a Plebe advisor is designated the team's Senior Plebe Advisor. Senior Plebe Advisors play several roles, including coordinating the activities for the team, as well as mentoring junior counterparts. For the Class of 2016 consisting of 1,200 midshipmen, a total of 85 faculty and staff members form the Plebe advising network. All Plebe advisors, including Senior Plebe Advisors, must attend a yearly training session held each summer in June prior to the start of Plebe Summer. During the session, all aspects of the Plebe curriculum are discussed. A Plebe Advisor's Handbook[6] is available on our intranet.

Once advisement training is completed in June, two important meetings occur between Plebes and their advisors during Plebe Summer. The first meeting, called the *Academic Counseling and Registration (ACR)* session, is an orientation meeting held in early July. At the ACR, midshipmen are introduced to the academic program in general, to various courses that they will be taking, and to their matrix of courses for the fall semester. In addition, results of validation exams are provided. The second meeting (that occurs in late July or early August) is the *Academic Advising and Study Skills (AA/SS) meeting*. At this meeting, more details about the academic program are discussed, but the focus is now shifted to academic readiness and performance. Tips for success, time management, and study skills dominate the topics in this two-and-a-half-hour session. Consequences of poor academic performance are discussed, and support programs to remedy poor performance are detailed. Plebes are provided an Academic Handbook[7] for reference.

After the fall semester has started, advisors schedule additional meetings to track academic performance: at one of three grading periods during the semester, to prepare

[5] All students (~4400) live in Bancroft Hall (USNA dormitory) and are organized into 30 Companies. The Company organization construct is a part of the military structure of USNA.
[6] http://intranet.usna.edu/AcCenter/docs.php
[7] http://intranet.usna.edu/AcCenter/docs.php

for pre-registration of spring courses, and to inform midshipmen of the majors from which they can select. In addition, Plebe open house tours for each program are held. These tours provide an opportunity for up-close introductions to a program.

In the second semester (beginning in January) of the Plebe year, Plebes select their academic major. The process starts with Plebe briefings, which are held in January. Organized similar to a conference, the briefings showcase programs and are the last promotions of particular programs prior to major selection. In March, before Spring Break, midshipmen select their academic majors. Midshipmen selecting the Cyber Operations Program are assigned to an academic advisor from among the faculty associated with the program.

These program-based faculty advisors, who take over upon return from Spring Break, come from either civilian or military faculty members associated with the Cyber Operations Program. Civilian faculty provide an academic, research-oriented and professional perspective, while the military faculty provide a useful perspective on the military career environment that graduates of the program will face. Both civilian and military faculty serve as formal advisers who are assigned to specific students (average of 10 students per Academic Adviser), and all faculty are generally informally accessible for advice – providing a supportive community for students to develop learning goals, plan courses and progress toward a naval career.

Communication between the midshipmen and their assigned program advisors varies according to the needs and to the desires of the individuals involved. The registration process for each semester occurs in two phases: a pre-registration phase and a registration phase. Pre-registration occurs the semester prior and is used to determine which courses and how many sections will be needed the following semester. Pre-registration data also provides information on student interest in major electives. Midshipmen are required to meet with their academic advisors to review academic progress and course selection prior to pre-registration. Course descriptions are available to the student in an on-line course listing[8] or from the online catalog[9].

Midshipmen then select courses to pre-register using the MIDS (Midshipmen Information System) program. Advisors are directed to review the status of their advisees using MIDS after pre-registration to ensure that perquisites have been met and course sequencing is correct. Once courses and the number of sections have been determined, students are directed to complete registration on MIDS to finalize their schedules. At this point sections are assigned, schedules are determined, and any problems are identified. In the latter case the advisor will be notified by the Registrar via the program's Senior Academic Advisor and will work with the advisee to resolve the problem.

As graduation approaches, the faculty advisor completes the initial review and verification of the midshipmen course of study. The advisor is aided in this task by MIDS, which enables the advisor to check the status of midshipmen course completion for general

[8] http://www.usna.edu/AcDean/courses/courses.html
[9] http://www.usna.edu/Catalog/

distribution requirements and for completion of required courses. The Naval Academy Registrar also performs an automated screening using MIDS and forwards the results to the Senior Academic Advisor for follow-up. The Senior Academic Advisor performs checks on all senior students to verify that they are all on track to graduate.

E. Work in Lieu of Courses

Summarize the requirements and process for awarding credit for work in lieu of courses. This could include such things as life experience, Advanced Placement, dual enrollment, test out, military experience, etc.

As stated previously, all midshipmen enter the Naval Academy as Plebes. For the core courses in mathematics, science, and humanities, students have the option to validate courses through examination during Plebe Summer, which is the summer preceding the fourth-class (freshman) year. The validation exams are administered and graded by their respective departments. Excellent performance on these placement exams may result in a midshipman validating a course, and thus accelerating portions of his/her academic program[10].

With regard to cyber operations, students have the opportunity to validate the introductory course (SY110). If a midshipman has taken similar course work at another institution, has a 4 or 5 on an AP Computer Science exam, or has had sufficient practical industrial experience, the student may request to sit for a validation exam for SY110. To be considered for validation credit a transcript of the grade and a course description from the previous institution, AP-examination documentation, or a detailed description of the relevant practical experience is required. The program's Senior Academic Advisor reviews each validation request to ascertain the scope and nature of the equivalent college-level academic or professional experience. If the Senior Academic Advisor judges the prior experience to be sufficient preparation, the student is allowed to sit for a validation exam at the discretion of the program administrator. Validation credit is considered for students with a written validation exam score of 80% or higher, and if required (for courses that include a significant amount of programming), a practical validation exam score of 80% or higher. To this point we have had only one validation for SY110.

F. Graduation Requirements

Summarize the graduation requirements for the program and the process for ensuring and documenting that each graduate completes all graduation requirements for the program. State the name of the degree awarded (Master of Science in Safety Sciences, Bachelor of Technology, Bachelor of Science in Computer Science, Bachelor of Science in Electrical Engineering, etc.)

All midshipmen follow a clearly defined program of study referred to as a *matrix*—the content of which depends on the student's major. The matrix for the Cyber Operations Program is shown in Table 1-3; a full program of study with course names is given in

[10] http://www.usna.edu/Academics/Candidate-Information/Course-Validation-Policy.php

Appendix E and in the Curriculum Section. All students are required to take a minimum of 15 credits every semester. Approval by the Associate Dean for Academic Affairs is required to take more than 23 credits. Progress through the matrix is monitored by the student's academic advisor and the Registrar. It is the advisors' responsibility to check that a student is on track, help the student choose appropriate courses each semester based on prerequisites and co-requisites, and ensure that the student registers for at least 15 credits. As students approach graduation, a check is made by the Registrar's Office, as well as the Senior Academic Advisor, to ensure that the student has met all requirements. In the event of an error, the Senior Academic Advisor for the program and the student's academic advisor are notified in time to correct the problem.

Table 1-3. Cyber Operations Matrix, Class of 2020.

	Freshman (4/c)		*Sophomore (3/c)*		*Junior (2/c)*		*Senior (1/c)*	
	Fall	*Spring*	*Fall*	*Spring*	*Fall*	*Spring*	*Fall*	*Spring*
Core	SC111-4	NS101-2	NE203-3	NN210-2	NN310-3	NL310-2	NL400-2	NS43*-2
	SM121-4	SC112-4	SP211-4	SP212-4	EE301-4	HM/SS2-3	ES300-3	EA/N4**-4
	HE111-3	SM122-4	SM223-4	HH216-3	HM/SS1-3		EM300-4	
	HH104-3	HE112-3	HH215-3	SM242-4				
	SY110-3	FP130-3						
		NL110-2						
Major			SY201-4	SY202-3	SY301-4	SY304-3	SY401-3	SY402-3
				SY204-4	SY303-4	SY306-3	SY403-3	SY406-3
						SY308-3	SY4**-3	SY4**-3
						SY310-4		
Credits	17	18	18	20	18	18	18	15

Credits are shown after each course. The * character denotes a wildcard.
Total credits hours = 142.

A cumulative grade-point average of 2.0 (C) on a 4.0 scale is required for graduation. A midshipman must also have a cumulative average of 2.0 (C) in those courses designated as part of the major in order to receive a degree designation on the transcript and diploma. If this criterion in the major courses is not met, then the degree is awarded as a Bachelor of Science with no other designation. This latter criterion grew out of the Final Statement from the 1999 ABET-EAC visit, which recommended that a minimum grade-point average be adopted for the engineering program. At the recommendation of the Faculty Senate, the criterion was endorsed for all academic majors at the Naval Academy and was approved by the Superintendent.

The degree awarded to those having a cumulative average of 2.0 (C) in the major is a Bachelor of Science in Cyber Operations.

G. Transcripts of Recent Graduates

The program will provide transcripts from some of the most recent graduates to the visiting team along with any needed explanation of how the transcripts are to be interpreted. **These transcripts will be requested separately by the Team Chair.** State how the program and any program options are designated on the transcript. (See 2017-2018 APPM, Section I.E.3.a.)

The program is designated on the transcript as Cyber Operations. There are no program options.

CRITERION 2. PROGRAM EDUCATIONAL OBJECTIVES

A. Mission Statement

Provide the institutional mission statement.

The Naval Academy's mission statement is as follows:

To develop midshipmen morally, mentally and physically and to imbue them with the highest ideals of duty, honor and loyalty in order to graduate leaders who are dedicated to a career of naval service and have potential for future development in mind and character to assume the highest responsibilities of command, citizenship and government.[11]

In addition, the Naval Academy Strategic Plan identifies the attributes of its graduates:[12]

Attributes of a Naval Academy Graduate

We graduate midshipmen who are warriors ready to meet the demands of a country at war or at peace. Our graduates are:

SELFLESS: Selfless leaders who value diversity and create an ethical command climate through their example of personal integrity and moral courage.

INSPIRATIONAL: Mentally resilient and physically fit officers who inspire their team to accomplish the most challenging missions and are prepared to lead in combat.

PROFICIENT: Technically and academically proficient professionals with a commitment to continual learning.

INNOVATIVE: Critical thinkers and creative decision makers with a bias for action.

ARTICULATE: Effective communicators.

ADAPTABLE: Adaptable individuals who understand and appreciate global and cross-cultural dynamics.

[11] http://www.usna.edu/mission.htm
[12] http://www.usna.edu/StrategicPlan/htmls/sp_graduates.html

PROFESSIONAL: Role models dedicated to the profession of arms, the traditions and values of the Naval Service and the constitutional foundation of the United States.

B. Program Educational Objectives

List the program educational objectives and state where these can be found by the general public.

Program Educational Objectives (PEOs) are defined as "Broad statements that describe the career and professional accomplishments that the program is preparing graduates to achieve."[13] The Cyber Operations Program's PEOs are as follows:

PEO 1 Applied skills and problem-solving abilities to solve Cyber-Operations-related Navy and Marine Corps problems.

PEO 2 Communicated effectively in both oral and written form about Cyber Operations to both technical and non-technical audiences.

PEO 3 Practiced the ethical, legal, and social implications of Cyber Operations consistent with Navy and Marine Corps core values (Honor, Courage, and Commitment[14]).

PEO 4 Grown through continuing education and professional development in Cyber Operations that is relevant to officers and scientists.

By five-to-seven years after graduation, we expect that our students will have achieved these PEOs. The Cyber Operations PEOs are available online.[15]

C. Consistency of the Program Educational Objectives with the Mission of the Institution

Describe how the program educational objectives are consistent with the mission of the institution.

Recall that the Naval Academy's mission is as follows:

To develop midshipmen morally, mentally and physically and to imbue them with the highest ideals of duty, honor and loyalty in order to graduate leaders who are dedicated

[13] *Criteria for Accrediting Computing Programs*, Effective for Reviews During the 2015–2016 Accreditation Cycle, ABET Computing Accreditation Commission.
[14] http://www.navy.mil/navydata/navy_legacy_hr.asp?id=193
[15] http://www.usna.edu/Cyber/peo.php

to a career of naval service and have potential for future development in mind and character to assume the highest responsibilities of command, citizenship and government.[16]

We now examine the consistency of the Cyber Operations Program's PEOs with various segments of the institutional mission statement.

To develop midshipmen morally …

The goal of developing midshipman morally is supported by PEO 3, because the proper ethical, legal, and social implications of computing are necessary for Naval Officers to employ cyber-operations methods and systems in a morally correct manner.

… leaders who are dedicated to a career of naval service …

All four PEOs support the goal of preparing graduates for the Naval services, since officers must be able to apply their skills to solve problems (PEO 1), communicate effectively (PEO 2), act morally (PEO 3), and further their professional development (PEO 4) in order to succeed in their military careers. Graduates of the Naval Academy will be entrusted with great responsibility to employ cyber-operations methods and systems both effectively and responsibly during their careers.

… to assume the highest responsibilities of command, citizenship and government.

PEOs 2, 3, and 4 support the goal of preparing midshipmen to assume the highest responsibilities of command, citizenship, and government because graduates are expected to continue their education and assume leadership roles in the public and private sectors after their military service, and many will inevitably be required to make decisions on the efficient and proper employment of cyber-operations technology.

In summary, it is clear that the Cyber Operations Program's PEOs strongly support the institution's mission.

D. Program Constituencies

List the program constituencies. Describe how the program educational objectives meet the needs of these constituencies.

There are four main constituencies of the Naval Academy's Cyber Operations Program:

- The operational forces of the military services (the employers of our graduates), primarily the US Navy and the US Marine Corps.
- The schools where our graduates seek advanced education. These primarily include, but are not limited to, the *Naval Postgraduate School (NPS),* Naval War College, Army War College, Air War College, Armed Forces Institute of Technology, and National Defense University.

[16] http://www.usna.edu/mission.htm

- Our students, the midshipmen majoring in the Cyber Operations Program.
- The faculty and staff who are teaching and working to support the Cyber Operations Program.

There are additional secondary constituencies, including the Naval Academy Alumni Association, the other Department of Defense and government agencies with whom our graduates may serve (for example, the National Security Agency [NSA], Defense Intelligence Agency [DIA], State Department, and so on), and ultimately the American taxpayers. These other groups sometimes provide input to the program but, for the purpose of formal assessment, we restrict our list of named constituencies to the four principal stakeholders. Note that our CCSS Board of Advisors is also a secondary stakeholder, and they provide a great deal of guidance and feedback to the program. Their inputs and assessment are detailed elsewhere in this Self-Study.

The following paragraphs examine how the PEOs meet the needs of each of our constituencies:

Military Services Constituency:

Not every graduate of the Cyber Operations Program will immediately and directly apply their academic skills on the battlefield, though many will. Graduates serve in a wide spectrum of roles as Naval Officers. They join the Surface Warfare, Submarine, Naval Aviation, Special Warfare, and Marine Corps (Infantry, Artillery, Armor, and so on) communities, for example, and many others. The PEOs meet the needs of the operational forces by ensuring graduates will be able to apply their skills and problem-solving abilities in an operational setting (PEO 1—applied problem solving), convey applied technology concepts to cyber-operations experts and to fellow service members (PEO 2—communication), and employ cyber-operations technology solutions in a legally and ethically responsible manner (PEO 3—legal, ethical, and responsible). In order to keep up with a rapidly changing area, our graduates must continue to grow and to increase their knowledge (PEO 4—continuing education and professional development).

Though the extent to which cyber operations methods and systems are employed will vary widely among the different warfare communities, the pervasiveness of cyber operations is increasing throughout each community. Some graduates will join the US Navy's *Information Professional* or *Cyber Warfare (IP/CW)* Officer communities, where they will more immediately employ their cyber-operations skill set.

Graduate Institutions Constituency:

Many graduates who remain on active duty beyond their initial period of obligated service (five years) will have an opportunity to attend one of the military graduate institutions listed previously. The Navy provides 1,600 funded opportunities each year for degree and non-degree programs that include 412 quotas at the Naval Postgraduate School, 180 quotas at top civilian universities, 242 quotas at the Naval War College, 379 quotas at Joint and other Service Colleges, 22 quotas at international military colleges, and 85 quotas dedicated to fellowship and training with industry.

The Naval Postgraduate School, in particular, provides graduate training for many officers in the Navy's IP/IW communities by way of the NPS Computer Science curricula. NPS also has a CS major track specific to Cyber Security which piggybacks nicely on our Cyber Operations Program. Whether our graduates eventually enroll at the Naval War College, Naval Postgraduate School, or elsewhere, a proper foundation in Cyber Operations, as supported by our Program Educational Objectives (PEO 4—continuing education) will be fundamentally important to their success. And, the capability our students to succeed in graduate school will depend heavily on their ability to perform well at (PEO 1—applied problem solving) and (PEO 2—communication).

Student Constituency:

By ensuring that the PEOs are met, the program contributes substantially to the institution's goals of producing high quality naval officers with the ideal attributes. Since all graduates spend at leave five years as naval officers, then the PEOs explicitly support the student constituency.

Faculty and Staff Constituency:

The Cyber Operations Program's faculty and staff need a framework to guide development of our courses of instruction, and the PEOs help fill this role. The faculty and staff need to know what material must be covered during a student's program in order to prepare that student for future attainment of the PEOs as a graduate. The PEOs help us to determine those elements of a student's proper educational foundation in Cyber Operations that will facilitate that student's success as a Naval Officer, years after graduation.

E. Process for Review of the Program Educational Objectives

Describe the process that periodically reviews the program educational objectives including how the program's various constituencies are involved in this process. Describe how this process is systematically utilized to ensure that the program's educational objectives remain consistent with the institutional mission, the program constituents' needs and these criteria.

The Cyber Operations Program PEOs are reviewed annually and approved by the Cyber Operations Program's Assessment Committee. This approval is based on inputs from the CCSS Board of (External) Advisors and by the faculty and staff associated with the Cyber Operations Program. These reviews examine both the attainment of the PEOs and appropriateness with respect to the institutional mission, the program constituent's needs, and the ABET Criteria. Any proposed changes to the PEOs are drafted by the Assessment Committee, and approved by a vote of the faculty and staff members associated with the Cyber Operations Program. These changes, their implementation, and any follow-up assessment is documented and recorded in the Cyber Operations Program's Assessment Binder that is maintained by the Cyber Science Department Chair.

The PEOs in their initial form were drafted and approved by the Assessment Committee, vetted by program leadership, and then brought to the faculty and staff associated with the Cyber Operations Program for discussion and approval. The initial PEOs were

approved and adopted in March 2014. The PEOs were last affirmed without change at the 31 October 2016 Assessment Committee Meeting, based on input from the various constituencies.

The specific process for review and revision of the PEOs is documented in the Google Drive folder belonging to the Assessment Committee, as is also maintained in the Google Drive folder that contains Policies and Procedures for the Cyber Science Department. This process involves:

1. Annual solicitation of inputs from the various constituencies – A request for inputs has been made to the following constituencies dated 16 May 2017:
    a. Academic Dean's Office
    b. Math and Science Division Director and Senior Professor
    c. Department Chairs with involvement in the major, including Computer Science, Electrical and Computer Engineering, and Weapons and Systems Engineering.
    d. Center for Cyber Security Studies and its External Advisory Board
2. Based on the inputs from (1), a new version of the PEOs will be ratified by the Assessment Committee and will become effective at the beginning of Fall semester of AY2018 (in August 2017).

CRITERION 3. STUDENT OUTCOMES

A. Student Outcomes

List the student outcomes for the program, including any outcomes that the program has defined beyond the required outcomes specified in the general criteria and any applicable program criteria.

Up until Spring AY2017, the following were the student outcomes for the program:

(a) An ability to apply knowledge of computing and mathematics appropriate to the discipline;

(b) An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution;

(c) An ability to design, implement and evaluate a computer-based system, process, component, or program to meet desired needs;

(d) An ability to function effectively on teams to accomplish a common goal;

(e) An understanding of professional, ethical, legal, security, and social issues and responsibilities;

(f) An ability to communicate effectively with a range of audiences;

(g) An ability to analyze the local and global impact of computing on individuals, organizations and society;

(h) Recognition of the need for, and an ability to engage in, continuing professional development;

(i) An ability to use current techniques, skills, and tools necessary for computing practices.

These “old” outcomes are enabled by the program in various courses as captured in Table 3-1 below.

Table 3-1 – Mapping of "old" SOs to Required SY Courses

SO	Required Cyber Operations (SY) Courses													
	110	201	202	204	301	303	304	306	308	310	401	402	403	406
a	X			X	X					X				
b		X			X			X						
c			X			X								
d	X										X	X		
e		X											X	X
f							X					X		
g							X						X	X
h		X												
i	X								X					

In Spring AY2017, the Assessment Committee changed the outcomes to the outcomes that are required by ABET under the pilot criteria.

1. An ability to analyze a problem, and to identify and define the computing requirements appropriate to its solution.
2. An ability to design, implement, and evaluate a computer-based solution to meet a given set of computing requirements in the context of the discipline.
3. An ability to communicate effectively with a range of audiences about technical information.
4. An ability to make informed judgments in computing practice based on legal and ethical principles.
5. An ability to function effectively on teams to establish goals, plan tasks, meet deadlines, manage risks and produce deliverables.
6. An ability to apply security principles and practices to the environment, hardware, software, and human aspects of a system.
7. An ability to analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats.

These "new" outcomes are enabled by the program in various courses as captured in Table 3-2 below.

Table 3-2 – Mapping of "new" SOs to Required SY Courses

SO	Required Cyber Operations (SY) Courses													
	110	201	202	204	301	303	304	306	308	310	401	402	403	406
1	X	X	X	X	X	X		X	X	X	X	X		
2	X	X	X	X	X	X		X	X	X	X	X		
3			X				X				X	X	X	
4							X				X		X	X
5							X				X	X	X	X
6	X	X		X	X	X	X	X	X	X	X	X	X	X
7	X							X		X	X	X	X	

B. Publication of Student Outcomes

Describe how the student outcomes are documented and publicly stated.

The outcomes are published on our public Web site at http://www.usna.edu/CyberCenter/Academics/so.php.

CRITERION 4. CONTINUOUS IMPROVEMENT

This section of your Self-Study Report should document your processes for regularly assessing and evaluating the extent to which the student outcomes are being attained. This section should also document the extent to which the student outcomes are being attained. It should also describe how the results of these processes are utilized to affect continuous improvement of the program.

Assessment is defined as one or more processes that identify, collect, and prepare the data necessary for evaluation. Evaluation is defined as one or more processes for interpreting the data acquired though the assessment processes in order to determine how well the student outcomes are being attained.

Although the program can report its processes as it chooses, the following is presented as a guide to help you organize your Self-Study Report.

A. Student Outcomes

It is recommended that this section include (a table may be used to present this information):

1. A listing and description of the assessment processes used to gather the data upon which the evaluation of each student outcome is based. Examples of data collection processes may include, but are not limited to, specific exam questions, student portfolios, internally developed assessment exams, senior project presentations, nationally-normed exams, oral exams, focus groups, industrial advisory committee meetings, or other processes that are relevant and appropriate to the program.
2. The frequency with which these assessment processes are carried out
3. The expected level of attainment for each of the student outcomes
4. Summaries of the results of the evaluation process and an analysis illustrating the extent to which each of the student outcomes is being attained
5. How the results are documented and maintained.

Because our program is new and cybersecurity is an emergent field, we are still experimenting with the best way to do assessment. The shift in ABET criteria and our two back-to-back reviews has placed this experimentation in the context of a moving target. As such, we report on two different assessment processes here. Process One was the process that we utilized for assessment prior to AY2017 (i.e., during AY2016 and before). Process Two was designed in AY2017 within the context of the revised outcomes (as they evolved in real-time), and implemented in Spring AY2017. Process Two reflects our assessment process as redesigned, and this is the process that will be followed for AY2018 and beyond. We report on Process One and Process Two separately below. The Process One text is mostly taken from our previous self-study that was used for our AY2017 General Criteria evaluation.

Process One

As noted above, the text in this section describes the assessment process that was in place through AY2016; this text is adapted with little change from the previous self-study from the AY2017 visit.

The assessment and continuous improvement processes for the Cyber Operations Program is managed by an Assessment Committee, working in concert with the Course Directors and Course Coordinators. The assessment committee meets at a minimum three times a year:

- Beginning of fall semester to verify assessment tools for the fall courses;
- End of fall/beginning of spring semester to validate fall course assessment forms and verify spring course assessment tools;
- End of the spring semester to validate spring assessment forms.

They also meet additionally as needed with the course coordinators to review assessment requirements and offer assessment improvements.

The Cyber Operations Program employs three primary assessment methods: *Graded Work, Student Opinion of Instruction, and Course Coordinator Reviews*. These are discussed below:

- *Graded Work*

  Table 3-2 shows a mapping between courses and the "old" SOs (for Process One). For each course in the table that corresponds to a specific SO Y, the instructors teaching the course (under the direction of the course coordinator) develop several pieces of graded work to measure Y. This graded work usually takes the form of specific homework, lab, quiz or exam questions. *Under Process One, each SO was regularly assessed using this approach.*

- *Student Opinion Form*

  At the completion of every course, each student fills out a SOF online, using a student login for authentication. SOFs are stored in a database[17] which is maintained by the Computer Science Department. Instructors can access the SOFs through an instructor login. SOFs are intended for use primarily by the instructor, but they are also reviewed by the respective Department Chair. The Chair will bring to the attention of the Assessment Committee anything that stands out from the norm. Again, this is not a direct measure of individual SOs, but is an important part of the assessment of our program.

- *Course Coordinator Reviews*

  At the end of the semester, each Course Coordinator fills out a Course Coordinator Review. This report includes an assessment of the offering, with recommendations. The Coordinator Review is especially useful in maintaining continuity when a course is turned over to a new instructor. Again, this is currently

[17] http://www.sof.cs.usna.edu/

not structured to directly assess individual SOs, but it does provide an important dimension to the overall assessment process. Though the information in the review is normally subjective, when appropriate, instructors are encouraged to include objective data that illustrates attainment of the SOs. Our intention is to enhance this measure in the future to require more definitive assessment of the SOs.

Table 4-1 below indicates basic information about each assessment measure, including items (1), (2), (3) and (5) as required by this section. Item (4) (the results of assessment cycles thus far) is discussed separately after the table.

Table 4-1-– Summary of Assessment Measures

Assessment Type	Direct/Indirect	Granularity	Frequency	Expected Level of Attainment	Basic Process
Graded Work (GW)	Direct	Measures each SO	Performed each time a course is taught that measures SOs (currently done in every course that maps to an SO from Table 3-2)	C+ proficiency on each measure.	Course coordinator collects SGW from the various instructors and computes the assessment metrics for the course. Results are given to the Course director and to the Assessment Committee. The Assessment Committee combines assessments from all courses to produce an evaluation result for each SO.
Student Opinion Form	Indirect	Measures quality of instruction only, based on standard institutional categories. Not based on specific SOs.	Performed for each course at the end of the course	No specific level, as results are confidential. However, specific problems are pointed out to the Course Director, Course Coordinator and/or the Assessment Committee, as appropriate.	Students complete online surveys, with results reported to the Cyber Science Department Chair. Anomalies are reported to the Assessment Committee.
Course Coordinator Reviews	Direct	Qualitative feedback on each course by the coordinators	Performed for each course at the end of the course	An issue the surfaces relative to an outcome is considered by the Course Director and the Assessment Committee for possible improvement	The Course Coordinator completes the course review and submits the results to the Course Director and to the Assessment Committee for further action.

With regard to item (4) from the outline (the degree to which the student outcomes are being attained), Table 4-2 summarizes the degree to which each outcome is being attained – based on the results of the specific graded work from each course (referred to as "GW" in the table below). (The outcomes in place in Table 4-2 were based on the previous "graduate attributes" in the CAC criteria labeled (a) through (i).)

Table 4-2 – Attainment of the Student Outcomes

Outcome	Measure Type	Last Measured	Measured Value	Attained?
(a) An ability to apply computing and mathematics appropriate to the discipline	SY 204 – GW (all labs for course)	Spring AY2016	5 of 7 Lab averages above 70%	Mostly attained; labs with lower scores will be refined
	SY 301 – GW (Project #3)	Fall AY2016	90%	Attained
	SY 310 – GW (Midterm – Q1/Q2)	Spring AY2016	80%/80%	Attained
	SY 310 – GW (Final – Practical)	Spring AY2016	86.5%	Attained
(b) An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution;	SY 201 – GW (Final Problem #1)	Fall AY2016	74.9%	Attained; improved.
	SY 301 – GW (Project #2)	Fall AY2016	88%	Attained
	SY 306 – GW (Project #1)	Spring AY2016	95.9%	Attained
	SY 306 – GW (Midterm/Final)	Spring AY2016	82.2%/81.06%	Attained

(c)	An ability to design, implement and evaluate a computer-based system, process, component or program to meet desired needs;	SY 202 – GW (Problem #1)	Spring AY2016	C+ = 2; 2.6	Attained
		SY 202 – GW (Problem #2)	Spring AY2016	C+ = 2; 3.1	Attained
		SY 202 – GW (Problem #3)	Spring AY2016	C+ = 2; 3.2	Attained
		SY 202 – GW (Problem #4)	Spring AY2016	C+ = 2; 3.0	Attained
		SY 303 – GW (Final Exam)	Fall AY2016	48.2%	Not attained; improvements were identified
(d)	An ability to function effectively on teams to accomplish a common goal;	SY 401 – GW (Project Peer Evals)	Fall AY2016	Ranged between excellent and very good; only a few exceptions in the "satisfactory" category.	Attained
		SY 402 – GW (Project Peer Evals)	Spring AY2016	Ranged between excellent and very good	Attained
(e)	An understanding of professional, ethical, legal, security, and social issues and responsibilities;	SY 201 – GW (Final Problem #4)	Fall AY2016	77%	Attained; improved.
		SY 403 – GW (Final Prob 1/2/3)	Fall AY2016	82.5%/86.43%/91.25%	Attained
		SY 406 – GW (Final Prob 2/6)	Spring AY2016	89.35%/92.65%	Attained
(f)	An ability to communicate effectively with a wide range of audiences;	SY 304 – GW (Final paper and presentation projects)	Spring AY2016	87.5% (paper) 90% (presentation)	Attained
		SY 402 – GW (Capstone project presentation grades)	Spring AY2016	87.11%	Attained
(g)	An ability to analyze the local and global impact of computing on individuals, organizations and society;	SY 304 – GW (Essay Questions)	Spring AY2016	89.84%/91.37%/84.47%	Attained
		SY 403 – GW (Final Prob 1/2/3)	Fall AY2016	82.5%/86.43%/91.25%	Attained
		SY 406 – GW (Paper P2/Final P5)	Spring AY2016	96.8%/89.65%	Attained
(h)	Recognition of the need for, and an ability to engage in, continuing professional development;	SY 201 – GW (Homework 38)	Fall AY2016	98.5%	Attained; excelled.
(i)	An ability to use current techniques, skills and tools necessary for computing practice.	SY 308 – GW (HW04/HW11/Proj)	Spring AY2016	96.55%/90.83%/93.62%	Attained
		SY 308 – GW (Final - 3 questions)	Spring AY2016	70.69%/75.17%/70.68%	Very marginal; improvements identified

Process Two

Process Two was developed during AY2017 in response to internal feedback regarding our assessment process, in combination with changes in the ABET criteria to reflect prescribed Student Outcomes.

Process Two breaks the Student Outcomes each into several key performance indicators. These performance indicators are either based on syntactic decomposition of the outcome, or items that appear to be implicitly a part of the outcome. It is actually the indicators that are individually measured within the various courses; successful attainment of all of the indicators associated with an outcome is generally taken to mean that the outcome is attained. Table 4-3 below reflects the coverage of the different indicators within the various courses. (Of course, the indicators associated with each course can be "rolled up" for each outcome, thus deriving Table 3-2.)

Table 4-3 – Indicator Coverage in SY Required Courses

		Required Cyber Operations (SY) Courses													
LEARNING OUTCOME	**INDICATOR**	**110**	**201**	**202**	**204**	**301**	**303**	**304**	**306**	**308**	**310**	**401**	**403**	**402**	**406**
1, 2	PROGRAMMING	X	X	X	X	X	X		X	X	X	X		X	
1, 2	DS & ALGORITHMS	X		X		X			X	X	X			X	
1, 2	SYSTEMS	X		X	X		X				X				
1, 2	NETWORKS	X			X				X		X	X		X	
1, 2	ARCHITECTURE	X					X								
1	ANALYSIS			X		X									
2	DESIGN		X	X	X	X	X			X	X	X		X	
2	IMPLEMENTATION		X	X	X	X	X		X	X	X	X		X	
2	EVALUATION			X		X	X		X	X	X	X		X	
3	VERBAL COMM							X				X	X	X	
3	WRITTEN COMM			X				X				X	X	X	
3	USE OF VISUALS							X				X		X	
4	LEGAL PRINCIPLES							X				X	X		X
4	ETHICAL PRINCIPLES							X				X	X		X
4	MAKE JUDGMENTS							X				X	X		X
5	TEAM DYNAMICS							X			X	X	X	X	X
6	HARDWARE SECURITY						X								
6	SW/DATA SECURITY	X	X		X	X	X		X	X	X	X		X	
6	HUMAN SECURITY	X				X		X				X		X	
6	ENVIRONMENT SECURITY	X						X				X		X	
6	CONFIDENTIALITY	X			X	X		X			X	X	X		X
6	INTEGRITY	X	X		X	X	X				X	X	X	X	X
6	AVAILABILITY	X				X					X	X	X		X
6	RISK	X						X		X		X	X	X	X
6	ADVERSARIAL THINKING	X	X		X	X	X	X			X	X	X	X	X
7	OFFENSIVE CYBER OPS	X							X		X	X	X		
7	DEFENSIVE CYBER OPS	X							X		X	X	X	X	

For Process Two, the assessment methods used are the same as Process One, with the primary method continuing to be Graded Work. The frequency of assessment will be managed by the Assessment Committee, but it is intended that for at least the first several years, every KPI will be measured annually in every course in which it occurs. This will help in the design and institutionalization of our program until the content starts to become more standardized.

We partially executed Process Two during Spring AY2017 and obtained data from Final Exam questions in specific areas. The results of this partial evaluation are in Table 4-4. Red values are below an "average" expectation of 80%; this threshold will be adjusted as we gain experience, and we also expect to measure whether metrics are showing improvement or decline as we gain experience. The results of these measures will be used to make improvements in the various courses during AY2018.

Table 4-4 – Spring AY2017 Assessment Results

		4/C	3/C Fall	3/C Spring		2/C Fall		2/C Spring				1/C Fall		1/C Spring	
LEARNING OUTCOME	**INDICATOR**	**110**	**201**	**202**	**204**	**301**	**303**	**304**	**306**	**308**	**310**	**401**	**403**	**402**	**406**
1, 2	PROGRAMMING	71.0%	NIF	78.0%	77.0%	NIF	NIF		86.0%	66.0%	NA	NIF		IP	
1, 2	DS & ALGORITHMS	NA		NA		NIF			89.0%	89.0%	80.0%			IP	
1, 2	SYSTEMS	NA		87.0%	76.0%		NIF								
1, 2	NETWORKS	78.0%							78.0%		77.0%	NIF		IP	
1, 2	ARCHITECTURE	NA					NIF								
1	ANALYSIS			86.0%		NIF									
2	DESIGN		NIF	NA	NA	NIF	NIF			NA	NA	NIF		IP	
2	IMPLEMENTATION		NIF	NA	NA	NIF	NIF		85.0%	NA	NA	NIF		IP	
2	EVALUATION			NA		NIF	NIF		86.0%	NA	63.0%	NIF		IP	
3	VERBAL COMM							NA				NIF	NIF	IP	
3	WRITTEN COMM			NA				NA				NIF	NIF	IP	
3	USE OF VISUALS							NA				NIF			
4	LEGAL PRINCIPLES							NA				NIF	NIF		86.0%
4	ETHICAL PRINCIPLES							NA				NIF	NIF		94.0%
4	MAKE JUDGMENTS							NA				NIF	NIF		93.0%
5	TEAM DYNAMICS							NA				NIF	NIF	IP	NA
6	HARDWARE SECURITY						NIF					NIF		IP	
6	SW/DATA SECURITY	87.0%	NIF		81.0%	NIF	NIF		88.0%	70.0%	NA	NIF		IP	
6	HUMAN SECURITY	95.0%						NA			34.0%	NIF		IP	
6	ENVIRONMENT SECURITY	NA						NA				NIF	NIF	IP	NA
6	CONFIDENTIALITY	87.0%			85.0%	NIF		NA			NA	NIF	NIF	IP	87.0%
6	INTEGRITY	NA	NIF		85.0%	NIF	NIF				NA	NIF	NIF	IP	NA
6	AVAILABILITY	NA				NIF					NA	NIF	NIF	IP	NA
6	RISK	NA						NA		NA		NIF	NIF	IP	NA
6	ADVERSARIAL THINKING	82.0%	NIF		94.0%	NIF	NIF	NA			NA	NIF	NIF	IP	NA
6	OFFENSIVE CYBER OPS	NA							98.0%		NA	NIF	NIF		
7	DEFENSIVE CYBER OPS	NA							88.0%		79.0%	NIF	NIF	IP	

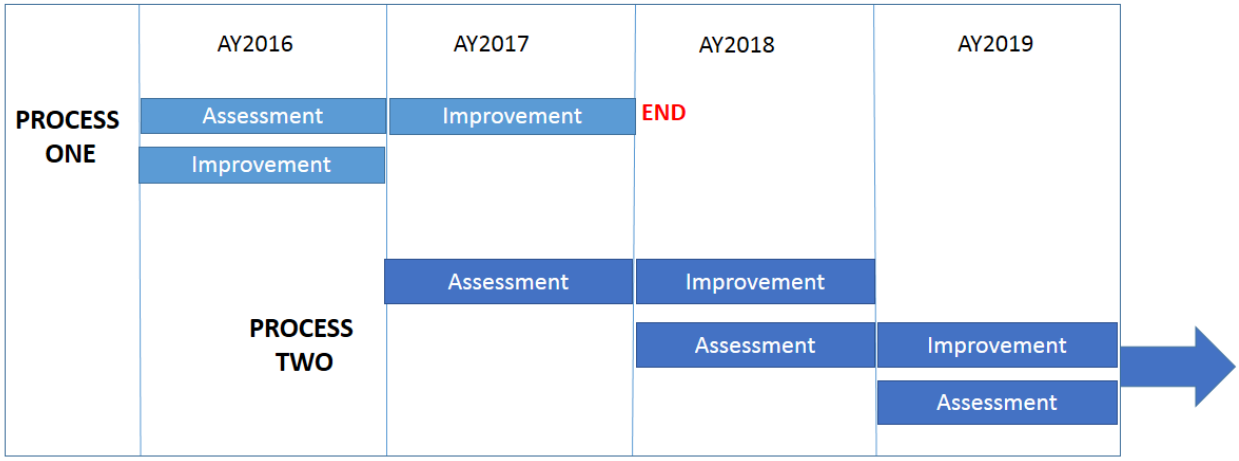
NA = Not assessed
NIF = Not implemented Fall AY2017 semester (was not implemented until Spring AY2017)
IP = In Progress (assessment results for SY402 are still being compiled)

B. Continuous Improvement

Describe how the results of evaluation processes for the student outcomes and any other available information have been systematically used as input in the continuous improvement of the program. Describe the results of any changes (whether or not effective) in those cases where re-assessment of the results has been completed. Indicate any significant future program improvement plans based upon recent evaluations. Provide a brief rationale for each of these planned changes.

We present continuous improvement also as "Process One" and "Process Two." Process One for assessment was executed through AY2016 inclusive, but from a continuous improvement perspective, the continuous improvement associated with an assessment cycle happened over the year following. Thus, for continuous improvement purposes, Process One includes the improvement cycle that took place during AY2017 (the year just finished). Process Two will then start with the improvement cycle in the upcoming academic year (AY2018). Figure 4-1 shows the transition between Process One and Process Two for both assessment and continuous improvement.

Figure 4-1 – Process One and Two Transition



Process One

As noted above, Process One was in place for continuous improvement through AY2017 inclusive. With regard to Process One, Table 4-1 shows an evaluation schedule for each of our three assessment measures, both in terms of timing and frequency. Through AY2016, those measures were conducted regularly according to the schedule identified in Table 4-1.

Under Process One, with regard to completing a formal assessment cycle for the SOs, the specific graded work was paramount, and generally followed this process:

1. (End of both AY semesters) Graded work was obtained from instructors and compiled by the Course Coordinators, who forwarded the results to the Assessment Committee.
2. (ASAP, but within 60 days) Assessment Committee reviewed all assessment data and formulated a report. Report is made to all Course Coordinators and Department Chair.
3. (Before next time the courses are taught) Course Coordinators made course improvements to prepare for next administration of the course, and provided improvements to Assessment committee in both the Course Assessment Tracking Form, and Course Coordinator Review Form.
4. Courses were then (re-)taught and the cycle repeats.

Based on the last assessment cycle belonging to Process One from AY2016 presented in Table 4-2, most of the metrics showed that the SOs were attained. Only a few of the metrics revealed a marginal or worse level of attainment. Based on the AY2016 assessment cycle, the following areas were targeted for improvement during AY2017:

Outcome	Course	Problem/Improvement
(a)	SY204	Labs with lower scores will be refined; both in the in-class instruction leading up to the lab and the lab content itself.
(c)	SY303	Students relied too heavily on 'practice exams' rather than course material. Future offerings will not provide practice exams and emphasize in-class material.

(i)	SY308	Give additional problem sets to improve the students' analysis skills. The exam problem may be too difficult for them to solve successfully, given the limited time. Make the exams shorter.

These items were implemented in AY2017 as part of the "improvements" portion of the cycle, and so far the results have been positive.

Previous assessment cycles have also resulted in improvements. Below are some of the changes that were implemented based on assessment results from previous cycles:

- Inheritance and Polymorphism not used in SY301 – Recommend removal from SY201
- Students were weak on Recursion. Recommend additional material on Recursion in SY201
- Student grades were low on the MD5 Lab. Instructors split the lab into two parts that focused on separate aspects of MD5 (Part1: Functions used in MD5, Little/Big Endian; Part2: MD5 Algorithm itself). Then they combined the work from both labs to recreate the entirety of the MD5 algorithm.
- SY301 course instructor reported that the students had a better understanding of recursion as a result of the changes
- Student average MD5 lab scores improved across the board, with more students submitting working code with an improved understanding of algorithms.

Process Two

The improvement portion of Process Two will be put in place for the AY2018 cycle. The continuous improvement portion of the cycle will be initiated from the Assessment Report for AY2017 that was recently completed based on the data in Table 4-4.

The following cycle is planned for Process Two beginning in 2017 and continuing to future years:

1. By June 1 each year, an Assessment Report will be produced by the Assessment Committee. This report will contain:
    a. A record of course improvements made during the previous year in response to previous assessment results (initially, the course improvements made during AY2017);
    b. The results of the assessment performed in the previous academic year (initially, in AY2017).
    c. Assessment plans for the upcoming year (initially, AY2018).
2. By mid-June[18], the Assessment Report is submitted to the Faculty Senate Assessment Committee (FSAC) for independent evaluation. Between mid-June and the beginning of the fall semester, the report is submitted to the Cyber Operations Program Faculty for consideration and planning of improvements.

[18] The FSAC reports are submitted on an institution-wide deadline, which is set to be approximately the last day of Spring semester appointments for 10-month faculty.

3. Over the upcoming academic year (initially, AY2018), improvements are executed in response to the Assessment Report. The Assessment Committee tracks these items and captures the improvements that were made in the following year report.
4. At the end of the academic year, assessment data are collected and used for the next annual report, at which point, the cycle resumes.

C. Additional Information

Copies of any of the assessment instruments or materials referenced in 4.A. and 4.B must be available for review at the time of the visit. Other information such as minutes from meetings where the assessment results were evaluated and where recommendations for action were made could also be included.

We will have an electronic summary of the last two assessment cycles (AY2016 and AY2017 assessment activities) available for review at the visit.

Future Improvements

We have identified a number of additional assessment tools that we would like to implement for the next academic year:

- *Midshipman Advisory Board*
  The MAB will consist of three-to-five Cyber Operations majors, typically one sophomore, two juniors, and two seniors. The MAB will meet with the Chair of the Cyber Science Department, the Associate Chair, the Assessment Committee Chair, and selected faculty members to provide verbal feedback on the most-recent course offerings. The student comments will be provided to faculty and staff members associated with the Cyber Operations Program in an anonymous format. The midshipmen will provide both positive and negative feedback, and suggestions for improvement. Although the feedback is not always specific to SOs, it will be useful in subjectively characterizing how effectively various topics are being presented in the Cyber Operations Program.
- *Graduating Senior Exit Survey*
  The Graduating Senior Exit Survey gives us feedback on the SOs from our graduating seniors. The survey will ask the graduating midshipmen to rate how well the Cyber Operations Program is enabling the SOs. For each SO a–i the midshipmen will be given the options Strongly Agree, Agree, Neutral, Disagree, and Strongly Disagree; the midshipmen will be asked to pick which answer they believe reflects whether the Cyber Operations Program enabled the given SO thereby allowing them to attain the SO. Survey results will be evaluated by the Assessment Committee.
- *Comprehensive Exam*
  There currently is no equivalent to the *Major Field Achievement Test (MFAT)* for Cyber Operations. We will develop an internal assessment exam that is designed to measure directly the level of student attainment of the SOs. The exam will be designed by the faculty members teaching in the Cyber Operations Program, and edited and approved by the Assessment Committee.

CRITERION 5. CURRICULUM

Note: *The following definitions are defied by CAC:*

One Academic Year *- For programs using standard semester units, one academic year is defined as 30 semester units. For programs using standard quarter units, one academic year is defined as 45 quarter units. For other programs, one academic year requires an equivalent amount of coursework.*

College-Level Mathematics *– College-level mathematics consists of mathematics above the pre-calculus level.*

A. Program Curriculum

1. Complete Table 5-1 that describes the plan of study for students in this program including information on course offerings in the form of a recommended schedule by year and term along with average section enrollments for all courses in the program over the two years immediately preceding the visit. **If there is more than one curricular path, Table 5-1 should be provided for each path.** State whether you are on quarters or semesters and complete a separate table for each option in the program.

The Naval Academy uses the semester system. There is only one option for completing the Cyber Operations Program. Students complete their studies using a course *matrix*. The following table shows the student matrix by semesters from left-to-right. The total numbers of credits per semester are shown at the bottom of the table, and each course's individual number of credits is shown next to it. Course names are given in Table 5-1.

4/C Fall	4/C Spring	3/C Fall	3/C Spring	2/C Fall	2/C Spring	1/C Fall	1/C Spring
SY110, 3	NS101, 2	NE203, 3	NN210, 2	NN310, 2	NL310, 3	NL400, 2	NS43X, 2
SC111, 4	NL110, 2	SP211, 4	SP212, 4	EE301, 4	HM SS2, 3	ES300, 3	EA/N4XY, 4
SM121, 4	SC112, 4	SM223, 4	SM242, 4	HM SS1, 3	SY304, 3	EM300, 4	SY402, 3
HE111, 3	SM122, 4	HH2XY, 3	HH216, 3	SY301, 4	SY306, 3	SY401, 3	SY406, 3
HH104, 3	HE112, 3	SY201, 4	SY202, 3	SY303, 4	SY308, 3	SY403, 3	SY4XY, 3
	FP130, 3		SY204, 4		SY310, 4	SY4XX, 3	
17	18	18	20	17	19	20	15

Table 5-1 Curriculum

Course (Department, Number, Title) List all courses in the program by term starting with first term of the first year and ending with the last term of the final year.	Indicate Whether Course is Required, Elective or a Selected Elective by an R, an E or an SE.[1]	*Subject Area (Credit Hours)*				Last Two Terms the Course was Offered: Year and, Semester, or Quarter	Average Section Enrollment for the Last Two Terms the Course was Offered[2]
		Math & Sciences	Computing Topics Mark with an F or A for Fundamental or Advanced	General Education	Other		
Year 1 F: Cyber Science, SY110, Introduction to Cyber Security I	R		3F			F17, S17	20.0
Year 1 F: Chemistry, SC111, Foundations of Chemistry	R	4				F16, F17	20.0
Year 1 F: Mathematics, SM121, Calculus I	R	4				F16, F17	20.0
Year 1 F: English, HE111, Rhetoric and Introduction to Literature I	R			3		F16, F17	20.0
Year 1 F: History, HH104, American Naval History	R			3		F16, F17	20.0
Year 1 S: Fundamentals of Seamanship, NS101, Introduction to Navigation	R				2	S16, S17	20.0
Year 1 S: Leadership, Ethics and Law, NL110, Preparing to Lead	R			2		S16, S17	20.0
Year 1 S: Chemistry, SC112, Foundations of Chemistry II	R	4				S16, S17	20.0
Year 1 S: Mathematics, SM122, Calculus II	R	4				S16, S17	20.0
Year 1 S: English, HE112, Rhetoric and Introduction to Literature II	R			3		S16, S17	20.0
Year 1 S: Political Science, FP130 , US Government and Constitutional Development	R			3		S16, S17	20.0
Year 2 F: Leadership, Ethics, and Law, NE203, Ethics and Moral Reasoning for the Naval Leader	R				3	F16, F17	20.0
Year 2 F: Physics, SP211, General Physics I	R	4				F16, F17	20.0
Year 2 F: Mathematics, SM223, Calculus III with Optimization	R	4				F16, F17	20.0
Year 2 F: History, HH215, The West in the Pre-Modern World	R			3		F16, F17	20.0
Year 2 F: Cyber Science, SY201, Cyber Fundamentals I	R		4F			F16, F17	20.0
Year 2 S: Seamanship and Navigation, NN210, Basic Navigation	R	1			1	S16, S17	20.0
Year 2 S: Physics, SP212, General Physics II	R	4				S16, S17	20.0
Year 2 S: Mathematics, SM242, Discrete Mathematics and Probability	R	4				S16, S17	20.0
Year 2 S: History, HH216, The West in the Modern World	R			3		S16, S17	20.0
Year 2 S: WSE, SY202, Cyber Systems Engineering	R		3F			S16, S17	20.0
Year 2 S: Computer Science, SY204, Sys Programming and Op Systems Fundamentals	R		4F			S16, S17	20.0

Year 3 F: Seamanship and Navigation; NS310, Advanced Navigation	R	1			1	F16, F17	20.0
Year 3 F: Electrical and Computer Engineering, EE301, Electrical Fundamentals and Applications	R	4				F16, F17	20.0
Year 3 F: Humanities, SS1, Social Science 1	SE			3		F16, F17	20.0
Year 3 F: Computer Science, SY301, Data Structures for Cyber Operations	R		4A			F16, F17	20.0
Year 3 F: ECE, SY303, Cyber Systems Architecture	R		4A			F16, F17	20.0
Year 3 S: Leadership, Ethics, and Law, NL310, Leadership: Theory and Applications	R				3	F16,F17	20.0
Year 3 S: Humanities, SS2, Social Science 2	SE			3		F17,S17	20.0
Year 3 S: Cyber Science, SY304, Social Engineering, Hacktivism, and Information Operations in Cyber	R		2F		1	S16,S17	20.0
Year 3 S: Computer Science, SY306, Web and Databases for Cyber Operations	R		3A			S16,S17	20.0
Year 3 S: Computer Science, SY308, Security: Fundamental Principles	R		3A			S16,S17	20.0
Year 3 S: ECE, SY310, Introduction to Networking and Wireless Communications	R		4A			S16,S17	20.0
Year 4 F: Leadership, Ethics, and Law, NL400, Law for the Junior Officer	R				2	F16,F17	20.0
Year 4 F: Weapons and Systems Engineering Department, ES300, Naval Weapons Systems	R				3	F17,S17	20.0
Year 4 F: Mechanical Engineering, EM300, Principles of Propulsion	R	4				F17,S17	20.0
Year 4 F: Cyber Science, SY401, Cyber Operations I	R		3A			F16, F17	20.0
Year 4 F: Cyber Science, SY403, Cyber Planning and Policy	R		1A		2	F16, F17	20.0
Year 4 F: [Various], SY4XY, Cyber Science Elective	SE			3		F16, F17	20.0
Year 4 S: Seamanship and Navigation, NS43X , Junior Officer Practicum	R				2	S16,S17	20.0
Year 4 S: Naval Architecture and Ocean Engineering, EA/N4XY, Principles of Ship Performance	R	2			2	F17,S17	20.0
Year 4 S: Cyber Science, SY402, Cyber Operations II	R		3A			S16, S17	20.0
Year 4 S: Cyber Science, SY406, Cyber Law and Ethics	R				3	S16, S17	20.0
Year 4 S: [Various], SY4XY, Cyber Science Elective	SE			3		S16, S17	20.0
TOTALS-ABET BASIC-LEVEL REQUIREMENTS		44	16F, 25A	35	25		
OVERALL TOTAL CREDIT HOURS FOR COMPLETION OF PROGRAM	142						

NOTE: "F15" means "Fall of AY2015" (or Fall of CY2014) – using the same convention as the rest of the document to denote academic terms.

1. **Required** courses are required of all students in the program, **elective** courses (often referred to as open or free electives) are optional for students, and **selected elective** courses are those for which students must take one or more courses from a specified group.
2. For courses that include multiple elements (lecture, laboratory, recitation, etc.), indicate the maximum enrollment in each element. For selected elective courses, indicate the maximum enrollment for each option.

Instructional materials and student work verifying compliance with ABET criteria for the categories indicated above will be required during the campus visit.

2. Describe how the curriculum aligns with the program educational objectives.

The program's four program educational objectives are as follows:

PEO 1 Applied skills and problem-solving abilities to solve Cyber-Operations-related Navy and Marine Corps problems.

PEO 2 Communicated effectively in both oral and written form about Cyber Operations to both technical and non-technical audiences.

PEO 3 Practiced the ethical, legal, and social implications of Cyber Operations consistent with Navy and Marine Corps core values (Honor, Courage, and Commitment[19]).

PEO 4 Grown through continuing education and professional development in Cyber Operations that is relevant to officers and scientists.

Each required course in the program has course learning objectives. Each required course supports at least one Student Outcome. Each syllabus shows a mapping of some course learning outcomes to Student Outcomes. The Student Outcomes are mapped to the program educational objectives as shown in Table 3-1 provided in Criterion 3, part B of this Self-Study. We elaborate further below.

Each of the four PEOs is supported directly by a number of courses in the curriculum. In particular, PEO 1 is supported by:

- SY110 (Introduction to Cyber Security)
- SY201 (Cyber Fundamentals I),
- SY202 (Cyber Systems Engineering),
- SY204 (Systems Programming and Operating Systems Fundamentals),
- SY301 (Data Structures for Cyber Operations),
- SY303 (Cyber Systems Architecture),
- SY304 (Social Engineering, Hacktivism, and Information Operations in Cyber), SY306 (Web and Databases for Cyber Operations),
- SY308 (Security: Fundamental Principles),
- SY310 (Introduction to Networking and Wireless Communications),
- SY401(Cyber Operations I), and
- SY402 (Cyber Operations II).

These courses are designed to teach applied skills and problem-solving abilities to solve Cyber-Operations-related Navy and Marine Corps problems. In Table 5-1 the "Other" column has a total of 22 credits, and many of these courses instruct students about issues in the military.

PEO 2 is directly supported by:

- SY204 (Systems Programming and Operating Systems Fundamentals),

[19] http://www.navy.mil/navydata/navy_legacy_hr.asp?id=193

- SY301 (Data Structures for Cyber Operations),
- SY304 (Social Engineering, Hacktivism, and Information Operations in Cyber), SY310 (Introduction to Networking and Wireless Communications), and
- SY402 (Cyber Operations II).

These course require students to learn about and practice communication in both oral and written forms.

PEO 3 is directly supported by:

- SY201 (Cyber Fundamentals I),
- SY304 (Social Engineering, Hacktivism, and Information Operations in Cyber),
- SY403 (Cyber Planning and Policy), and
- SY406 (Cyber Law and Ethics).

These courses teach ethical, legal, and social implications of Cyber Operations consistent with Navy and Marine Corps core values.

PEO 4 is directly supported by:

- SY201 (Cyber Fundamentals I),
- SY204 (Systems Programming and Operating Systems Fundamentals),
- SY301 (Data Structures for Cyber Operations),
- SY310 (Introduction to Networking and Wireless Communications), and
- SY402 (Cyber Operations II).

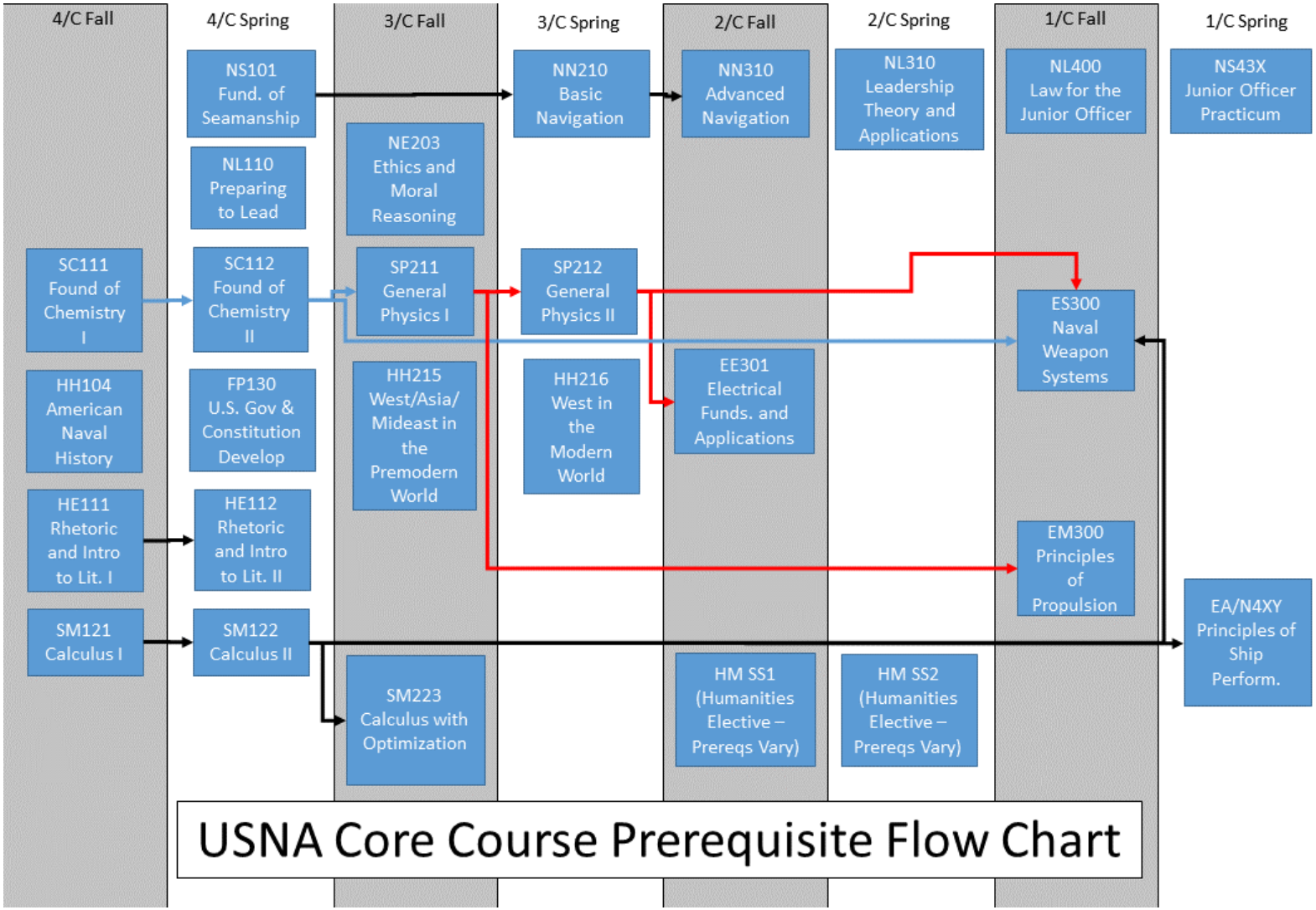
These courses teach about continuing education and professional development opportunities in Cyber Operations that is relevant to officers and scientists.

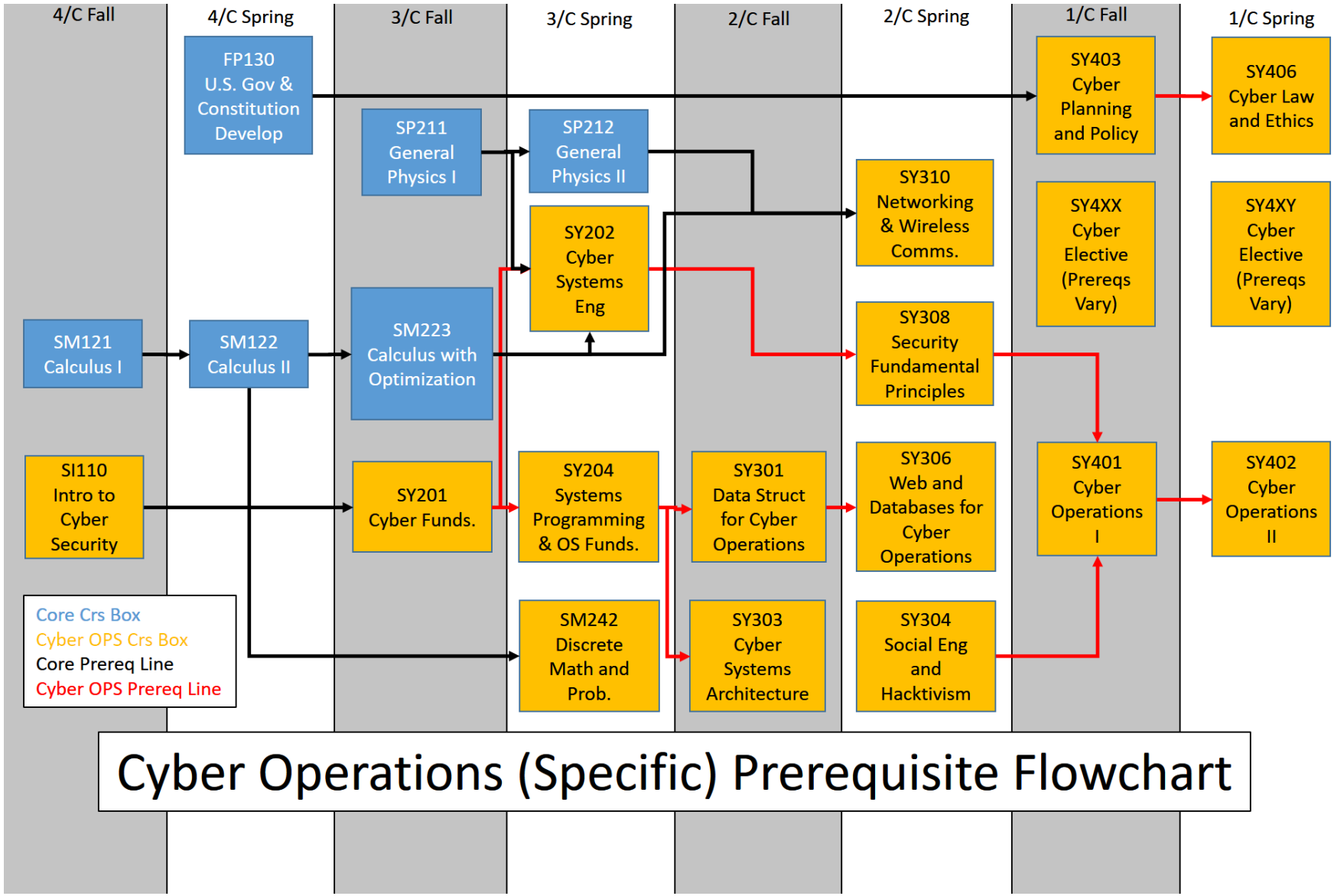
Thus, the curriculum prepares the midshipmen well to achieve the program educational objectives during the next phase of their careers.

3. Describe how the curriculum and its associated prerequisite structure support the attainment of the student outcomes.

Both the old set and new set of student outcomes are mapped to the required courses in the program. The old set of student outcomes is mapped to the required courses in Table 3-1. The new set of student outcomes is mapped to the required courses in Table 3-2. Mapping an outcome to a course means that the outcome is "covered" in that course. For example, Old Student Outcome (h) "Recognition of the need for, and an ability to engage in, continuing professional development" is supported in SY201 (Cyber Fundamentals I), where lectures are given about the need for and the opportunities to participate in continuing professional development. Students are then asked to complete homework that consists of a series of questions related to continuing professional development. The homework is graded and discussed with the students. Other Student Outcomes are enabled in a similar manner throughout the curriculum. The prerequisite structure is designed to make sure that the midshipmen have both the required background to complete more-advanced topics and the required maturity.

4. Attach a flowchart or worksheet that illustrates the prerequisite structure of the program's required courses.




4/C Fall
4/C Spring
3/C Fall
3/C Spring
2/C Fall
2/C Spring
1/C Fall
1/C Spring
FP130 U.S. Gov & Constitution Develop
SP211 General Physics I
SP212 General Physics II
SY403 Cyber Planning and Policy
SY406 Cyber Law and Ethics
SY202 Cyber Systems Eng
SY310 Networking & Wireless Comms.
SY4XX Cyber Elective (Prereqs Vary)
SY4XY Cyber Elective (Prereqs Vary)
SM121 Calculus I
SM122 Calculus II
SM223 Calculus with Optimization
SY308 Security Fundamental Principles
SI110 Intro to Cyber Security
SY201 Cyber Funds.
SY204 Systems Programming & OS Funds.
SY301 Data Struct for Cyber Operations
SY306 Web and Databases for Cyber Operations
SY401 Cyber Operations I
SY402 Cyber Operations II
Core Crs Box
Cyber OPS Crs Box
Core Prereq Line
Cyber OPS Prereq Line
SM242 Discrete Math and Prob.
SY303 Cyber Systems Architecture
SY304 Social Eng and Hacktivism
Cyber Operations (Specific) Prerequisite Flowchart

5. For each curricular area specifically addressed by either the general criteria or the applicable program criteria as shown in Table 5-1, describe how your program meets the specific requirements for this program area in terms of hours and depth of study.

   There are no applicable program criteria, as the program is being evaluated under the General Criteria only. The following narrative describes how the program meets Criterion 5.

   Technical and Professional Requirements

   The curriculum does combine technical and professional requirements (85 credits) with general education requirements and electives (57 credits) that prepare students for a professional career and further study in a computing discipline. The program prepares students to function in modern society, as they graduate up-to-date on the most-important issues relating to cyber security.

   The program requires a total of 41 credits of up-to-date fundamental and advanced topics in cyber operations. This amount is substantially more than the one year required by the Criterion 5.

   Mathematics Appropriate to the Discipline and Beyond the Pre-calculus Level

   The program requires the following four 4-credit courses that provide 16 credit hours of mathematical background for the technical courses:

   SM121— Calculus I
   SM122 — Calculus II
   SM223 — Calculus III with Optimization
   SM242 — Discrete Math and Probability

   Note that all of these courses are beyond the pre-Calculus level.

6. If your program allows cooperative education to satisfy curricular requirements specifically addressed by either the general or program criteria, describe the academic component of this experience and how it is evaluated by the faculty.

   The program has no cooperative education component.

7. Describe the materials (course syllabi, textbooks, sample student work, etc.), that will be available for review during the visit to demonstrate achievement related to this criterion. (See the 2014-2015 APPM Section II.G.6.b. (2) Regarding display materials.)

   For each required course in the Cyber Operations Program a physical binder will be available that contains the course syllabus, samples of graded student work, and

other relevant materials for that course, for example, quizzes, mid-term examples, homework assignments, labs, projects, and final exam. For courses that require a textbook a copy of the textbook will be provided in the display room.

In addition to the physical materials, electronic access will be provided to course materials where feasible. Both course and assessment materials will be provided electronically where feasible. Electronic access will be provided subject to the following considerations:

1. USNA's campus network is behind a firewall that only exposes a portion of its Web footprint. Course Websites, with only a few exceptions, are generally entirely behind the firewall and are only available for access while physically on campus, or through a VPN client.
2. About 2/3 of our courses have basic Websites available straight through http or https. The other 1/3 of course Websites are implemented through Blackboard. Those sites, while available to the students in the courses, are not available to the visiting team. However, materials from those sites will be electronically mirrored to the team for the purposes of the visit, via Dropbox.
3. USNA uses Google Apps for Education, and is a significant user of Google Drive to share documents across the enterprise for instructional purposes. The Cyber Science Department uses Google Drive to share departmental policies and procedures, as well as assessment data and reports where documentation is required. References to storage of documents within particular Google Drive directories take place throughout this document; such directories are shared among departmental faculty and relevant constituencies through directory sharing within Google Drive. While the team cannot be provided direct Google Drive access, the Google Drive materials will be mirrored to the team via Dropbox.

B. Overall Course Management and Staffing

As noted previously, all courses in the Cyber Operations Program are managed by Course Directors and Course Coordinators, with Course Directors responsible for long term course management, and Course Coordinators responsible for short term operational course management within a given semester. The table below lists the Course Directors and Course Coordinators for our required major courses for AY2018 alongside each individual's organization (CYS for Cyber Science Department, CCSS for Center for Cyber Security Studies, WSE for Weapons and Systems Engineering Department, ECE for Electrical and Computer Engineering Department and CS for Computer Science Department).

Course Number	Course Director	Course Coordinator
SY110	Hoffmeister (CYS)	Hoffmeister (CYS)
SY201	Parrish (CYS)	Shumba (CYS)
SY202	Rodriguez-Seda (WSE)	Rodriquez-Seda (WSE)
SY204	Hoffmeister (CYS)	Hoffmeister (CYS)
SY301	Mayberry (CYS)	Mayberry (CYS)
SY303	Brown (CYS)	Brown (CYS)
SY304	Hatfield (CYS)	Hatfield (CYS)
SY306	Crainiceanu (CS)	Crainiceanu (CS)
SY308	Mayberry (CYS)	Mayberry (CYS)
SY310	Gardner (ECE)	Gardner (ECE)
SY401	Orr (CYS)	Orr (CYS)
SY402	Kenney (CS)	Kenney (CS)
SY403	Inglis (CYS)	Inglis (CYS)
SY406	Kosseff (CYS)	Kosseff (CYS)

C. Course Syllabi

In Appendix A, include a syllabus for each course used to satisfy the mathematics, science, and discipline-specific requirements required by Criterion 5 or any applicable program criteria.

CRITERION 6. FACULTY

A. Faculty Qualifications

Describe the qualifications of the faculty and how they are adequate to cover all the curricular areas of the program and also meet any applicable program criteria. This description should include the composition, size, credentials, and experience of the faculty. Complete Table 6-1. Include faculty resumes in Appendix B.

Academy Wide

The composition of the faculty at the Academy is fairly unique in that it consists of a roughly even blend of civilians and military officers. Navy is committed to funding USNA to ensure a 50-50 faculty mix with 50% of the faculty being civilian professors with a terminal degree in their field and 50% military professors and instructors with at least master's degrees. We refer to this as the 294/294 plan with 294 civilian faculty and 294 military faculty. In the past several years, we have largely met the 294 civilian faculty number, but we have not yet met the 294 military instructor mark due to the phased nature of the plan to increase the number of military instructors.

Civilian tenure/tenure track faculty members hold a terminal degree in their respective fields and have active research programs in addition to their teaching duties. Rank and tenure are awarded and held in a manner consistent with what is typical among major comprehensive and liberal arts universities across the United States. Junior faculty members are hired as untenured at the Assistant Professor level and typically spend 6 years in rank prior to tenure and promotion to Associate Professor. Promotion to Professor is based on criteria specified within the Faculty Handbook requiring success in teaching, research and service. There is a Yard-wide Faculty Promotion and Tenure Committee that hears all academic promotion and tenure cases.

Civilian faculty also includes "visiting" faculty drawn from a variety of sources – including faculty on sabbatical from other institutions, and loaned faculty from DoD and other agencies, including NSA. There is also a Distinguished Visiting Professor (DVP) program for scholars of world-renown stature to be in residence. All of these civilian faculty members are very highly qualified.

With regard to the military faculty, there are four types of officer professor/instructors, primarily coming from a variety of Navy warfare specialties (most typically surface line, submarines, and aviation, and Marines). All officers bring the benefit of their operational experience with them into the classroom. The four types of officer professor/instructors are as follows.

Permanent Military Professors (PMP). PMPs are Senior Naval Officers with PhDs in their field of expertise. Officers who have achieved the rank of Commander (CDR) can apply for the PMP program. If selected, they are sent to graduate school to obtain a Ph.D. and return to teach at USNA until mandatory retirement (typically 28 years for an officer at the rank of CDR or 30 years for those who attain the rank of CAPT). Unlike the rotational military faculty, these PMP officers are required to continue their research and are expected to publish while at USNA. Additionally, PMP officers can apply for untenured

academic promotions and are reviewed by the same promotion and tenure committee that evaluates civilian professors.

Junior Permanent Military Professors (J-PMP). J-PMPs are mid-level officers who have master's degrees in their field of expertise. Naval Officers with approximately 10 years of service who have achieved the rank of Lieutenant Commander (LCDR) can apply for the Junior-PMP (J-PMP) program. These officers hold MS degrees and teach at USNA until mandatory retirement (typically 20 years for an officer at the rank of LCDR). Unlike the PMP officers, J-PMPs are not expected to publish while at USNA.

Rotational Officers. Rotational officers are officers that are assigned to the Academy on a multi-year rotational basis. Rotational officers typically serve for two to three years at a time and are not required to conduct research. However, they are assigned significant additional military duties such as participation in midshipmen summer cruise activities, acting as military representative for sports teams, extracurricular activities, or other midshipmen training activities. One of the most important duties of the rotational military faculty is to bring their military experience into the classroom to help the midshipmen develop professionally and to point out how the subject matter applies to their military careers. Since the rotational military faculty serve for only a few years, the civilian or permanent military faculty members are responsible for maintaining program continuity. One major advantage of having the frequent turnover of military faculty is that they are generally fresh from their graduate education and infuse the department with new ideas. Rotational faculty all have MS degrees.

Inter-Service Exchange Officers. These officers are similar to rotational officers (described above), but are from a different service (typically from the US Air Force). These officers provide many of the benefits of rotational officers, but provide the perspective of a different service.

<u>Faculty Directly Supporting the Program</u>

The faculty with *primary* responsibility to the program are either in the Cyber Science Department (CYS) or the Center for Cyber Security Studies (CCSS). Outside of CYS and CCSS, for the upcoming Fall AY2018 semester, four of our course coordinators are from three other departments: Computer Science (CS), Electrical and Computer Engineering (ECE) and Weapons and Systems Engineering (WSE). These four coordinators are critical to the program, but are only partially allocated to the Cyber Operations program, as they also support programs in their home departments. Note that additional faculty from these other departments may also periodically teach in the program, depending on specific course demands. All faculty that teach in the program are well-qualified and fall into one of the categories described. In a small number of cases, adjunct faculty may be employed to teach sections of SY110.

Table 6-1(a) contains counts of the number of faculty in various institutional categories, spread among the various organizational units, and counting course coordinators housed outside of either CYS or CCSS. Because the exact number is a moving target, we provide "X/Y" – where "X" is the number of faculty in AY2017 and Y is the expected number of faculty in AY2018. Table 6-1 then contains detailed qualifications for the AY2017 faculty group, and it is those faculty members for which vitas are provided in Appendix B. Table

6-1 will be updated prior to the visit and additional vitas provided for AY2018 faculty who were not at USNA in AY2017.

Table 6-1(a): Number of Faculty Supporting the Program (AY17/AY18)

Department	PMP	JPMP	Other Mil	Civilian	Total
Cyber Science Department	0/0	3/3	0/2	7/6	10/11
Center for Cyber Security Studies	0/0	0/0	3/4	5/5	8/9
Electrical and Computer Engineering	0/0	0/0	0/1	0/0	0/1
Computer Science	0/0	1/1	0/0	1/1	2/2
Weapons and Systems Engineering	0/0	0/0	0/0	1/1	1/1
Total	0/0	4/4	3/7	14/13	21/24

Table 6-1(a) shows 18/20 (AY17/AY18) faculty with primary commitment to the program, and 21/24 (AY17/AY18) faculty that we regard as critical to the program. It should be noted that the Cyber Science Department also has two (2) PMPs currently enrolled in PhD programs (not currently contributing to the teaching program) and three (3) open civilian positions for which it is actively recruiting. This effectively adds five *potential* positions to the 20 with primary commitment to the program in Fall AY2018 – for a total of 25 *positions* allocated to the program.

B. Faculty Workload

Complete Table 6-2, Faculty Workload Summary and describe this information in terms of workload expectations or requirements (for the year of the Self Study).

Table 6-2 contains a workload analysis for the faculty supporting the program in AY2017.

Civilian faculty members generally teach no more than four days a week and therefore have at least one day a week in which to focus on research and other scholarly activities. Faculty teaching load is based on contact hours per academic year (Fall and Spring terms). For example, one section of a 2-2-3 course (2 recitation hours, 2 lab hours, 3 credit hours) is considered 4 contact hours (2 recitation plus 2 lab). Faculty loading ranges between 18 to 24 contact hours per academic year, with promotion and tenure track faculty (civilian P&T, PMP) towards the lower end of the scale and non-promotion and tenure track faculty (J-PMP, rotational military) towards the higher end of the scale. A section typically has 20 students in it, as most classrooms and labs are designed to fit 20 students with one instructor. A section must have at least 10 students to count towards teaching load. Sections with less than 10 students are considered an overload for the faculty member; independent research courses commonly fit this designation.

The department collateral duty assignments are reviewed annually by both the department chair and the associate chair. The department chair assigns collateral duties based in large part on the needs of the department, faculty interest, as well as their projected teaching and research loads. The department chair then makes additional adjustments throughout the year, as necessary, to support the arrival and departure of rotational military faculty and any unforeseen major shifts in the time commitments of the faculty. Tenure-track faculty are afforded increased opportunities to pursue their

research as the rotational and junior military will take on increased collateral and administrative responsibilities.

C. Faculty Size

Discuss how the faculty serving in the program are of sufficient number to maintain continuity, stability, oversight, student interaction, and advising for the program.

The combined faculties of the Center for Cyber Security Students (CCSS) and the Cyber Science Department (CYS) provide the majority the management and leadership of the program. For the upcoming academic year, these combined faculties contain a total headcount of 20, with an additional 3 vacancies that are part of a civilian faculty search within the department to take place as soon as possible (as well as 2 additional PMPs who have been assigned to the program, but are currently obtaining PhDs in preparation for teaching). Three courses (SY202, SY306, SY310 and SY402) are directed and coordinated by (four) faculty members from outside of CCSS and CYS; these faculty members should be included among those providing oversight of the program.

Thus, there are effectively 25 positions allocated to the program at the level of "primary commitment" and an additional 4 faculty members from other departments providing curricular oversight. In addition, the departments of Computer Science, Weapons and Systems Engineering and Electrical and Computer Engineering contribute an additional headcount of approximately 10 individuals teaching approximately 20 sections of 6 different courses – this contribution has been relatively stable and accounted for in the resource allocations within these related departments. A few sections of SY110 in Spring AY2018 will likely be taught by adjunct faculty, and a couple of sections of SY201 are being taught by Dean Andrew Phillips and Associate Dean Peter Nardi – both of whom have relevant computing academic backgrounds.

With 20 core faculty (and a commitment of 25 positions) within the Department and Center, less than 150 students in the major, and with all section sizes less than or equal to 20 students – we feel that the sufficiency of the faculty size is self-evident. All faculty provide direct interaction with their students in class as well as academic advising and extra instruction. While allied computing-related departments (such as Computer Science) supply a small percentage of the overall instruction, that percentage is small and resource allocation for those other departments includes consideration for the support of the Cyber Operations program.

D. Professional Development

Provide detailed descriptions of professional development activities for each faculty member.

All faculty members are afforded the opportunity to travel to attend conferences, symposiums, and workshops both to present papers as well as to develop themselves professionally. Faculty members are encouraged to participate as reviewers and on program committees for journals and conferences and similar activities. See the

individual faculty vitae later in this document for specific activities of each faculty member.

E. Authority and Responsibility of Faculty

Describe the role played by the faculty with respect to course creation, modification, and evaluation, their role in the definition and revision of program educational objectives and student outcomes, and their role in the attainment of the student outcomes. Describe the roles of others on campus, e.g., dean or provost, with respect to these areas.

The program faculty in Table 6-1 is responsible for creating, evaluating and maintaining all courses required by the Cyber Operations major. Each course is managed by a Course Director (a faculty member with long term responsibility for the course) and a Course Coordinator (a faculty member responsible for the administration of a course during a given semester). Course Directors are relatively permanent, while Course Coordinators may rotate from semester to semester. In general, Course Directors serve as Course Coordinators if they are teaching the course that semester.

The faculty at USNA is extremely engaged in teaching, and all faculty members are heavily involved in their courses. The Course Director ensures that a course is institutionalized and the content is maintained – and also ensures that each course is constantly subject to assessment and continuous improvement. Effectively, Course Directors provide stability and strategic leadership for their courses. Course Coordinators, on the other hand, provide tactical leadership within a given semester for the administration of their courses. Course Coordinators also coordinate among multiple sections to ensure consistency of content and schedule, as well as to make sure that assessment activities are carried out.

Table 6-1. Faculty Qualifications

Cyber Operations Program[20]

Faculty Name (Organization)	Highest Degree Earned (Field and Year)	Acad Rank [1]	Type of Academic Appointment[2]	FT or PT[3]	Years of Experience			Professional Registration/ Certification	Level of Activity[4] H, M, or L		
					Govt./Ind. Practice	Teaching	This Institution		Professional Organization	Professional Developmen	Consulting/summer work in industry
Brown, Dane (Cyber Sci)	MS, Electrical and Comp Eng, 2010	I	NTT	FT	7	7	7		M	H	M
Crainiceanu, Adina (CS)	PhD, Computer Science, 2006	ASC	T	FT	12	12	12	GIAC	M	H	M
Debels, Mark (CCSS) (visiting from NSA)	MS, Computer Science, 1994	O	NTT	FT	23	2	2		L	H	H
Deckert, Benjamin (CCSS)	MS, Information Warfare Systems Eng, 2011	I	NTT (M)	FT	18	2	2		L	M	H
Devos, Dan (CCSS)	MS, IT Management, 2004	I	NTT(M)	FT	22	3	3		L	M	H
Hatfield, Joseph (Cyber Sci)	PhD, Political Science, 2015	AST	NTT (M)	FT	15	2	2	Six Sigma	L	H	L
Hoffmeister, Christopher (Cyber Sci)	MS, Comp Science, 2007	I	NTT	FT	15	5	5	Numerous	L	H	L
Inglis, John "Chris" (CCSS)	MS, Comp Science, 1984	DVP	NTT	PT	40	6	5	TS/SCI	L	H	H
Kenney, Jeffrey (Comp Sci)	MS, Comp Science & Informatics, 2015	I	NTT	FT	15	2	2	IWO/SWO	L	H	L
Kosseff, Jeffrey (Cyber Sci)	JD, Law, 2010	AST	TT	FT	15	4	2	CIPP, Bar	L	H	M
Lewis, James (CCSS)	PhD, Political Science, 1984	DVP	NTT	PT	33	5	1		H	H	H
Libicki, Martin (CCSS)	PhD, Economics, 1978	DVP	NTT	FT	30	7	5		L	H	H
Marinelli, Augustine (CCSS)	MA, Political Science, 2009	I	NTT(M)	FT	9	3	3		L	H	L
Mayberry, Travis (Cyber Sci)	PhD, Computer Science, 2015	AST	TT	FT	3	5	1	IACR / IFCA	M	H	L
Odunukwe, Yasmin (Cyber Sci)	MS, Engineering Management, 2011.	I	NTT	FT	12	1	1	DAWIA	L	M	L
Orr, Stephen (Cyber Sci) (visiting from NSA)	PhD, Cybersecurity, 2004.	O	NTT	FT	13	1	1		M	H	H
Parrish, Allen (Cyber Sci)	PhD, Computer Science, 1990	PROF	T	FT	27	27	1		H	H	M
Rodriguez-Seda, Erick (Sys Eng)	PhD, Electrical and Comp Engineering, 2011	AST	TT	FT	1	5	3		L	M	L
Roth, John (Cyber Sci)	PhD, Electrical Engineering, 2016	AST	TT	FT	12	4	4		M	H	H
Shumba, Rose, (Comp Sci)	PhD, Computer Science, 1995	PROF	TT	FT	20	20	1		M	H	M
Slack, Andrew (CCSS)	MS, Computer Science, 2009	I	NTT(M)	FT	13	3	3	IWO, GIAC	L	H	L
Tortora, Paul (CCSS)	MS, Nat'l Security and Strategic Stud., 2006	I	NTT	FT	28	5	5		M	M	H

Code: P = Professor, ASC = Associate Professor, AST = Assistant Professor, DVP = Distinguished Visiting Professor, I = Instructor, A = Adjunct, O = Other (Note: Hatfield has an academic rank of Assistant Professor as a military officer because of his (unusual) PhD as a JPMP.)
Code: TT = Tenure Track, T = Tenured, NTT = Non Tenure Track, NTT(M) = Non Tenure Track (Military)
Code: FT = Full-time, PT = Part-time Appointment at the institution
The level of activity, high, medium or low, should reflect an average over the year prior to the visit plus the two previous years.

Table 6-2. Faculty Workload Summary

Cyber Operations Program[21]

Faculty Member (name)	PT or FT	Classes Taught (Course No./Credit Hrs.) Term and Year[2]	Program Activity Distribution[3]			% of Time Devoted to the Program[5]
			Teaching	Research or Scholarship	Other[4]	
Brown, Dane (Cyber Sci)	FT	(SY303/4) Fall AY2017; (SY204/4) Spring AY2017	50%	50%		100%
Crainiceanu, Adina (Comp Sci)	FT	(SY306/3) Spring AY2017	100%			15%
Debels, Mark (Cyber Sci)	FT	(SY110/3 X 2) Fall AY2017; (SY204/4; SY110/3) Spring AY2017	80%	20%		100%
Deckert, Benjamin (CCSS)	FT	(SY110/3 X 2) Fall AY2017; (SY110/3 X 2) Spring AY2017	60%		40%	100%
Hatfield, Joseph (Cyber Sci)	FT	(SY110/3 X 2, FP407/3) Fall AY2017; (SY110/3 X 2, SY304/3) Spring AY2017	80%		20%	100%
Hoffmeister, Christopher (Cyber Sci)	FT	(SY201/4) Fall AY2017; (SY204/4) Spring AY2017	50%		50%	100%
Inglis, John "Chris" (CCSS)	PT	(SY304/3) Spring AY2017; (SY403/3) Fall AY2017	100%			25%
Kenney, Jeffrey (Comp Sci)	FT	(SY401/3) Fall AY2017; (SY402/3) Spring AY2017	100%			33%
Kosseff, Jeffrey (Cyber Sci)	FT	(SY403/3, SY486B/3, FP130/3) Fall AY2017; (SY406/3) Spring AY2017	80%	20%		100%
Lewis, James (CCSS)	PT	(SY304/3) Spring AY2017;	100%			15%
Libicki, Martin (CCSS)	FT	(SY486A/3) Spring AY2017; (SY110/3) Fall AY2017	60%	40%		100%
Marinelli, Joseph (CCSS)	FT	(SY304/3, SY110/3 X 2) Spring AY2017; (SY110/3 X 3) Fall AY2017	80%		20%	100%
Mayberry, Travis (Cyber Sci)	FT	(SY201/4, SY486C/3) Fall AY2017; (SY308/3, SY110/3) Spring AY2017	80%	20%		100%
Odunukwe, Yasmin (Cyber Sci)	FT	(SY110/3) Fall AY2017; (SY110/3) Spring AY2017	80%		20%	100%
Orr, Stephen (Cyber Sci)	FT	(SY401/3, SY110/3) Fall AY2017; (SY402/3, SY110/3 X 2] Spring 2018	80%	20%		100%
Parrish, Allen (Cyber Sci)	FT	(SY110, 3) Fall AY2017	50%		50%	100%
Rodriguez-Seda, Erick (Sys Eng)	FT	(SY202/3 X 2) Spring AY2017	100%			25%
Roth, John (Cyber Sci)	FT	(SY310/4 X 2) Spring AY2017	50%	50%		100%
Slack, Andrew (CCSS)	FT	(SY201/4) Fall AY2017; (SY401/3) Fall AY2017; (SY204/4) Spring AY2017; (SY402/3) Spring AY2017	60%		40%	100%
Shumba, Rose (Cyber Sci)	FT	(SY110/3 X 2) Fall AY2017; (SY110/3 X 2; SY486B/3) Spring AY2017	80%		20%	100%
Tortora, Paul (CCSS)	FT	(SY110/3) Spring AY2017	50%		50%	100%

1. Code: FT = Full-time, PT = Part-time Appointment at the institution
2. For the academic year for which the Self-Study Report is being prepared.
3. Program activity distribution should be in percent of effort in the program and should total 100%.
4. Indicate sabbatical leave, etc., under "Other."
5. Out of the total time employed at the institution.

[21] Faculty noted above in the Cyber Science Department are fully allocated to the program. Faculty from other units are allocated to the program based on the percentage of their overall effort that they teach in the program. Faculty from departments other than Cyber Science who are partially allocated to the program are shown as 100% teaching because their research and other duties are not part of the time they are devoting to the program.

CRITERION 7. FACILITIES[1]

A. Offices, Classrooms and Laboratories

Summarize each of the program's facilities in terms of their ability to support the attainment of the student outcomes and to provide an atmosphere conducive to learning.

1. Offices (such as administrative, faculty, clerical, and teaching assistants) and any associated equipment that is typically available there.

a. Faculty: Range from independent offices to cubicles within a common area. In cases where office space is shared, there is opportunity to move to a private conference room for confidential discussions related to grades and similar concerns. Each faculty member is issued an institution laptop, monitor, and peripherals.

b. Technical Staff: Staff generally share office space, but are issued institution laptop, monitor, and peripherals. Some have extra administrator accesses to institution servers in order to perform their duties.

c. Administrative Staff: Each admin personnel (called Education Technicians at USNA) generally sit at the front of the Department Chair's office to greet guests and visitors. They each have an issued desktop or laptop, monitor, peripherals, and licenses to software to support their duties (Adobe Pro, etc.).

2. Classrooms and associated equipment that are typically available where the program courses are taught.

Classrooms: Classrooms vary by size, but all generally are from 700 – 1050 sq.ft. Each has individual desks for the students, Wi-Fi access, and a hard-wired instructor desktop connected to a projector. Classrooms will either have chalkboards or whiteboards. Computer Labs will have department-owned desktops available for the students with identical software and OS load outs.

3. Laboratory facilities including those containing computers (describe available hardware and software) and the associated tools and equipment that support instruction. Include those facilities used by students in the program even if they are not dedicated to the program and state the times they are available to students. Complete Appendix C containing a listing of the major pieces of equipment used by the program in support of instruction.

Laboratory Facilities: All midshipmen are issued standard Windows laptops. The specifications for the laptops belonging to the Class of 2020 are given in Appendix E. These laptops are generally quite adequate for the majority of in-class and out-of-class

work for the Cyber Operations courses. In addition, there are a number of special purpose labs:

- War Room: 20 workstations, 10 laptops, mixed OS: Windows 8.1, Debian x64, Mac OS X; not tied to specific course, supports Faculty/MIDN research, supports MIDN Extra Curricular Activities, managed by Cyber Science, Leahy 300.
- Linux Labs: 3 Ubuntu x64 labs, 20-22 student workstations, 1 instructor workstation, managed by Computer Science, Michelson 302, Michelson 303, Michelson 316.
- Windows Lab: 1 Windows 7 Enterprise lab, 20-22 student workstations, 1 instructor workstation, managed by Computer Science, Michelson 392.
- Networking Lab: 1 Ubuntu x64 lab, ~60 Raspberry Pi's, 20-22 student workstations, 1 instructor workstation, other networking equipment, managed by Computer Science, Michelson 300.
- SCADA Lab: Various SCADA/ICS controllers, workbenches setup/arranged for small group work ~4 students section of ~20 students, managed by Systems Engineering, Maury 111.
- Computer Engineering Lab: Various Electrical Engineering and Computer Engineering equipment (oscilloscope, etc.), workbenches setup/arranged for pair work section of ~20 students, managed by Electrical and Computer Engineering, Rickover 065.
- Various Dependent on Elective: System Engineering Lab, Computer Engineering Lab, Robotics Lab, located in either Maury, Rickover or Michelson.

In addition to the above labs, we have recently stood up a virtual environment consisting of 2x Intel Xeon E5-2650 v3 2.3GHz10C/20T; 256GB RDIMM 2.133GHz; separate SAN. This will be utilized in various courses next year.

Building Information

Currently the Cyber Science Department and the Center for Cyber Security Studies are located in Leahy Hall. No courses are taught in Leahy, and there is only one laboratory facility there (the War Room). Most courses within the program are taught in Michelson Hall. Leahy Hall is serving as temporary housing for the CCSS and Cyber Science Department until the completion of a new $120M Cyber Operations building at the beginning of AY 2020. All of the disciplines and organizations contributing to the Cyber Operations Program will be fully housed in this building – including CCSS, Cyber Science, Computer Science, Electrical and Computer Engineering, and Systems Engineering.

B. Computing Resources

Describe any computing resources (workstations, servers, storage, networks including software) in addition to those described in the laboratories in Part A, which are used by the students in the program. Include a discussion of the accessibility of university-wide computing resources available to all students via various locations such as student housing, library, student union, off-campus, etc. State the hours the various computing facilities are open to students. Assess the adequacy of these facilities to support the scholarly and professional activities of the

students and faculty in the program.

Students have 24/7 remote access to all UNIX laboratory workstations via a secure (SSH) login from any host on the Naval Academy network, including their own PC in their dormitory room and from PCs located in the library. Similar broadband remote access to files in their Windows account is made possible via a network shared drive. The amount of computers, servers, and software both within the department and campus-wide is sufficient for the program.

C. Guidance

Describe how students in the program are provided appropriate guidance regarding the use of the tools, equipment, computing resources, and laboratories.

The department maintains a computing system support webpage on the USNA intranet which serves as a central point of guidance regarding the department's computing resources and laboratories. This webpage contains instructions for installing and using the various systems available to students in the program. Additionally, instructors provide course specific guidance via the course website. The students can also email or arrange to meet in person with the department's computing support staff for help as needed.

D. Maintenance and Upgrading of Facilities

Describe the policies and procedures for maintaining and upgrading the tools, equipment, computing resources, and laboratories used by students and faculty in the program.

Laboratory and computing resources are maintained with a life-cycle management process. Each year the department prepares an Abbreviated System Decision Paper (ASDP). The ASDP lists the department's system needs for the current fiscal year and seven following years; i.e. eight total fiscal years, the fiscal year is from October 1 to September 30. These items include: lab machines, faculty and staff workstations, printers, specialized hardware (e.g. drones, Raspberry Pi's), and faculty research equipment. Every set number of years (four years for workstations and servers) equipment is planned for replacement in the ASDP.

Funding is attached to support the ASDP request from four different sources:

- Enterprise (central administration) Funding – Supports permanent courses, printers, and faculty/staff workstations.
- Department Funding – Supports prototype/trial courses and provides $10,000 in startup funds to purchase equipment to support research efforts.
- Gift Funding – Currently through the CCSS, and supports equipment that is "over and above" what the enterprise and department can support to sustain a "margin of excellence" for cyber security education.
- Research Funding – Funding from research grants received by faculty can be used to purchase specialized research equipment.

The ASDP is submitted up the academic chain of command and to the Information Technology Services Division (ITSD) each fiscal year. (ITSD is the enterprise computing unit for the academy, and is under the direct management of the Superintendent.) Department leadership meets with ITSD financial managers to further discuss the ASDP after submission. Based on the ASDP and available funds, the department leadership prepares a prioritized list of purchases for the fiscal year and submits this list to the Academic Dean and Provost's Office for ranking across all academic units. The Academic Dean & Provost's Office then provides the finalized priority list to ITSD, which runs the information technology Life Cycle Management (LCM) program and allocates assets as required. ITSD evaluates the ASDP and approves each request based on timeliness and fit with other program and institutional priorities.

The Life Cycle Management process has proven to be effective in ensuring that laboratory and computing resources are replaced within the useable lifetime of each component item. The LCM is used by all departments across the institution, and remains capable of providing state of the practice equipment for student education and research. Additionally, there are substantial gift funds[22] available to provide a margin of excellence above state of the practice equipment.

E. Library Services

Describe and evaluate the capability of the library (or libraries) to serve the program including the adequacy of the library's technical collection relative to the needs of the program and the faculty, the adequacy of the process by which faculty may request the library to order books or subscriptions, the library's systems for locating and obtaining electronic information, and any other library services relevant to the needs of the program.

The United States Naval Academy is served by Nimitz Library. One of the library's staff reference bibliographers, Mr. Larry Clemens, is assigned the collateral duty of liaison to the Cyber Science Department. In this role, the Cyber Science library liaison selects materials for the Nimitz collection to support the teaching and research needs of the department, provides customized library instruction, and assists midshipmen and faculty with their individual research projects. The Cyber Science library liaison interacts with a member of the Cyber Science Department faculty to determine what additions, modifications or removals from the library services and subscriptions are needed by the department. The electronic journals available through Nimitz Library include: ACM Digital Library, Directory of Open Access Journals, IEEE Digital Library, IEEE Electronic Library Online, IEEE Spectrum Online, MIT Press Journals and Safari Tech books. The library also participates in an Interlibrary Loan and Document Delivery program. Overall, the Cyber Science Department has been able to obtain the books, technical documents, online resources, and other materials it needs from the USNA library.

[22] In CY2016 Lockheed Martin committed a multi-year general Cyber gift totaling $1.35M that will be spent over the next 5 years.

F. Overall Comments on Facilities

Describe how the program ensures the facilities, tools, and equipment used in the program are safe for their intended purposes. (See the 2017-2018 APPM section I.E.5.b.(1).)

There is no hazardous material contained in the department spaces or used in the program. All computing equipment is plugged into appropriate surge protector equipment.

CRITERION 8. INSTITUTIONAL SUPPORT

A. Leadership

Describe the leadership of the program and discuss its adequacy to ensure the quality and continuity of the program and how the leadership is involved in decisions that affect the program.

The leadership of the program comes from the CCSS and the Cyber Science Department. The Director of the CCSS is Paul Tortora; the Deputy Director is LCDR Andrew Slack (turnover of the Deputy Director is anticipated for Fall AY2018). These positions carry a three-year appointment.

The Chair of the Cyber Science Department is Dr. Allen Parrish, and the Associate Chair is LCDR Chris Hoffmeister (turnover of the Associate Chair is anticipated for Fall AY2018, although LCDR Hoffmeister will remain in the department and will be Chair of the Curriculum Committee). The Director of the CCSS reports directly to the Academic Dean & Provost Andrew Phillips, while the Chair of the Cyber Science Department reports to the Director of the Math and Science Division (currently CAPT David Roberts), who in turn reports to the Academic Dean and Provost. The structure of the Academic leadership is shown in Figure 1.

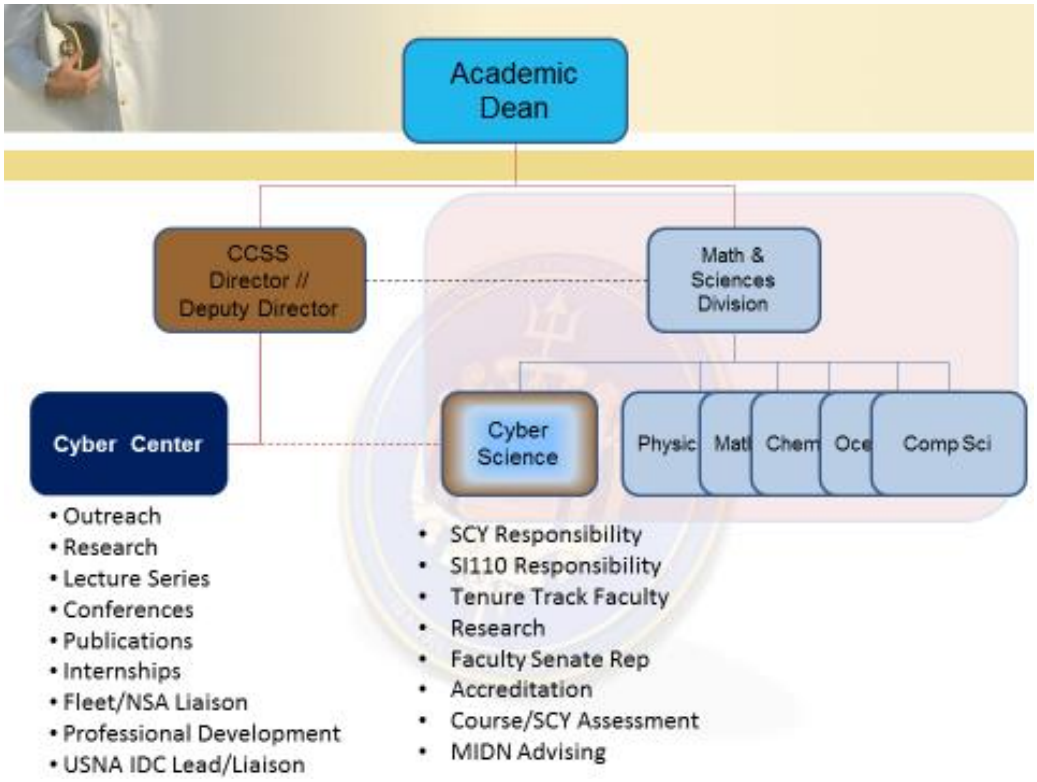


Figure 1. United States Naval Academy Academic Organization.

As noted in Figure 1, the CCSS is focused primarily on outreach to external constituencies, while the Cyber Science Department is focused primarily on the management of the faculty and curriculum. Such a bifurcated structure pushes many external and outreach responsibilities to the CCSS and allows the Departmental leadership more time to manage the faculty and curriculum. This is proving to be an effective model.

Among its external activities, the CCSS has been extremely effective in fundraising for the program, permitting the program to achieve a margin of excellence not otherwise possible. The program has benefitted tremendously from these resources, and the Cyber Science Department has been able to focus on providing the curriculum in the context of extraordinary resources - without having to take time away from the program to obtain those resources. As a result, the CCSS and the Department have been able to initiate an extremely positive, symbiotic relationship.

The above structure allows the Academic Dean and Provost to provide leadership for both internal and external aspects of the program. This means that Academy leadership is involved in decisions related to the program, curriculum, faculty, external constituencies and resources. The Academic Dean and Provost has provided energetic leadership for the program and in promoting cyber security as an area of emphasis for the institution.

In addition to the leadership provided via the Academic Dean and Provost, the CCSS also brings an independent Board of Advisors to the program as an important external leadership constituency. Members of the Board are some of the top cyber security professionals in academia, government and industry - and include Dennis Blair, Chris Inglis, Rick Ledgett, Robert Murrett, David Gompert, Gene Spafford, Lin Wells, Terry Roberts, William Lynn, Paul Speer, Lawrence Caviola, and Martin Libicki. The Board was formed in 2011. This group meets twice per year and has provided extensive input and guidance to the program throughout its development. The CCSS also has several distinguished professor positions, and these senior professors are able to provide additional leadership to the program.

Finally, the Superintendent of the Academy (analogous to a civilian college President) has made cyber security one of his three top institutional priorities. This has provided credibility and support for the program, and enabled the program to take root and grow substantially. The combination of this vision - along with leadership by the Academic Dean and Provost, as well by the Board of Advisors – has created enormous opportunity for this program to get started, become institutionalized, and ultimately achieve national and international prominence.

B. Program Budget and Financial Support

1. Describe the process used to establish the program's budget and provide evidence of continuity of institutional support for the program. Include the sources of financial support including both permanent (recurring) and temporary (one-time) funds.

Funds for faculty and staff salaries (including adjuncts) are managed centrally by the Academic Dean & Provost's Office. The Academic Dean & Provost works closely with the Division Director and Chair to determine the need for faculty and adjunct faculty based primarily on their teaching loads and on the needs for specific technical expertise. Rotational military faculty can also be shifted from one program to another to meet teaching requirements at the discretion of the Academic Dean & Provost and Division Directors. Because this program is a top institutional priority, we anticipate new positions to be added over the next 5 years until we have reached approximately 20 faculty members within the Cyber Science Department, alongside the faculty from other departments who will still be involved in delivering the program. With a steady state expectation of around 180 majors, this level of staffing should be quite adequate to deliver a quality program over the long term.

Funds provided to the Cyber Science Department and to the CCSS come from two primary sources: (a) appropriated funds that are part of the institution's budget and (b) gift funds that have been provided for use to promote the cyber security mission at USNA. *These gift funds have grown to be quite large, and are more than sufficient to support cyber security education at the Academy over the next 5 years at a very high level of excellence.* Through both of these funding sources, the program has been extremely well-supported by the Academy, and is in a great position to grow and excel over the next few years. Travel funds to support faculty development through conference travel and training have been more than sufficient for the needs of the program. Laboratory and classroom equipment have been well funded, and faculty have state-of-the-practice equipment for use for instruction and research. Because of the importance of our mission, we anticipate continued strong support from appropriated funds, and with a center (CCSS) dedicated to external outreach and working with potential funding donors, we anticipate continued success in obtaining gift funding to support the program.

One clear sign of evidence that the institution is providing outstanding support for the program is in the $120 million dollar, 206,000 square foot Cyber Building. As noted above, the building is projected to be completed in AY20, and will house CCSS, Cyber Science, Computer Science, Electrical and Computer Engineering, and Systems Engineering – all disciplines that substantially contribute to the Cyber Operations degree program. The new building will include labs, offices, classrooms, lecture halls, an observatory, salt-water wave tank, and a rooftop multipurpose space. The structure will be the first at the Naval Academy to include a *Sensitive Compartmented Information Facility (SCIF)* that will be used to allow midshipmen to handle classified information for research and to attend classified lectures.

2. Describe how teaching is supported by the institution in terms of graders, teaching assistants, teaching workshops, etc.

The Naval Academy does not use graders due to its small class size, and the belief that professors should be the ones who grade student work. All classes in the Cyber Operations Program have at most twenty midshipmen. We do use the *Midshipmen Group Study Program (MGSP)* to support teaching, and the Naval Academy has an

established infrastructure to help run this program. Professors typically recommend their previously enrolled top students from a course to participate in this program to support the given course. A student in MGSP will work closely under a professor's guidance to conduct review sessions for the midshipmen in one of the professor's classes. In the weekly sessions the MGSP leader and assistants will review homework, conduct study sessions prior to exams, conduct make-up labs, and answer any questions that midshipmen might have about a course. The students participating in MGSP are the closest thing that the Naval Academy has to teaching assistants, but all students participate on a voluntary basis.

The Naval Academy provides onsite teaching workshops on a regular basis through the Office of Faculty Development. These workshops are typically held prior to the summer intersession and during the winter break. ITSD (the enterprise computing unit for the academy) also conducts workshops for various software applications. And, the Naval Academy has required annual training for all of its faculty members and staff requiring things such as safe guarding information, sexual harassment prevention, and so forth. These sessions support the teaching mission.

3. To the extent not described above, describe how resources are provided to acquire, maintain, and upgrade the infrastructures, facilities, and equipment used in the program.

Described fully above.

4. Assess the adequacy of the resources described in this section with respect to the students in the program being able to attain the student outcomes.

The resources have been more than sufficient to enable the SOs. All midshipmen are issued high-quality laptops, and our classrooms and lab equipment for the program are excellent. All faculty members have state-of-the-art equipment, and the labs are well equipped.

C. Staffing

Describe the adequacy of the staff (administrative, instructional, and technical) and institutional services provided to the program. Discuss methods used to retain and train staff.

We handle each type of staff separately in our response to this section.

Administrative Staff: The Cyber Operations Program has a single shared administrative-staff position—an *educational technician*. The educational technician executes general administrative duties within the program, facilitates some acquisition and supplies, assists with curricular administrative tasks, and also provides critical support to sponsored travel.

There is a standardized campus-wide training that is required for secretaries and educational technicians. This training, which covers procedures such as payroll and travel, is required upon being hired and periodic refresher training is required. In addition, there are many annual required online training courses, for example, sexual-harassment prevention training, handling sensitive information, and so forth. We try to maintain a collegial environment in order to retain staff members.

The Cyber Science Department has a Chair and an Associate Chair that both manage and support the program. Reduced teaching loads are provided for both of these individuals.

Instructional Staff: The Cyber Operations Program is housed in the Cyber Science Department. As indicated previously, the faculty members teaching in the program come from a number of different programs, and some are housed in the Cyber Science Department or in the CCSS. A justification of the adequacy of the instructional staff was provided in the Faculty section.

In terms of instructional staff training, we typically assign mentors to new instructors. The faculty mentors describe the basic mechanics of working at USNA, MIDS, our teaching goals, how the CCSS and department operate, extra instruction (similar to office hours for students), and the teaching philosophy within the program. Other items such as research and funding expectations are discussed as well. New faculty members can meet with their mentors at any time, but they do meet at least once per semester during their first year. In addition, all new instructors at the Naval Academy undergo an extensive orientation session. Besides the initial training, each year faculty members complete annual training on a variety of topics.

Further, the Chair of the Cyber Science Department (as part of the oversight of the Cyber Operations Program) meets regularly with faculty members teaching in the Program. If there are any issues that come up, the Chair addresses those on an individual basis. We also work to retain faculty members by having a good collegial working environment. All of the faculty members are focused on doing what is best for the midshipmen, and this common goal helps with faculty retention. In the case of temporary military faculty members, they rotate out every three years. The incoming replacement military faculty members usually bring a great deal of energy and enthusiasm to the program, and many of them graduated from the Naval Academy. The opportunity to teach at their alma mater is a real honor and homecoming.

Technical Staff: Technical staff that support the program come from two sources: (a) the Information Technology Services Division (ITSD) already presented in the previous section, and (b) personnel employed directly by the various academic units. ITSD is the central enterprise computing support organization for the Academy, and its personnel are commonly referred to as Information Technology (IT) Specialists; these are professional staff members with IT backgrounds who support the academic program outside of the classroom (i.e. they are not present in a class during class time). Technical staff employed directly within the academic departments are commonly referred to as IPAs (Instructor of Practical Applications); these are also

professional staff members with IT backgrounds, but they are present in the classroom during class time in support of the faculty instructor of the class, hence the inclusion of "Instructor" in their title. Of the units supporting the Cyber Operations Program, Cyber Science, Systems Engineering, Electrical and Computer Engineering, and CCSS are all supported by IPAs. Computer Science, however, is supported entirely by IT Specialists from ITSD. This model has worked reasonably well, although ITSD staffing levels sometimes fluctuate and Unix support periodically has to be supplemented by assistance from qualified computer science faculty members.

D. Faculty Hiring and Retention

1. Describe the process for hiring of new faculty.

Once authorized by the Academic Dean & Provost to hire a new faculty member we oversee the hiring process. The program advertises nationally in the appropriate journals, other publications, and electronic venues. The Academic Dean & Provost provides some financial assistance to the program to help offset the costs of advertising and interviewing. We use a hiring committee to screen applicants and invite an appropriate number of applicants to visit the Naval Academy for a full-day interview. We usually interview between three and five applicants for an open position. We determine the most-appropriate candidates based on these interviews. We then request permission to hire our most-desirable candidate.

The Naval Academy strives to make competitive offers to new assistant professors in order to attract high-quality candidates. Further, the Naval Academy promises new faculty start-up research equipment and full salary coverage for their first three summers to assist faculty members with the establishment of a productive research program.

2. Describe strategies used to retain current qualified faculty.

One way the program tries to retain current qualified faculty is through strong support of newly hired members. Administrative and service demands on newly hired assistant professors are kept to a minimum in the first few years to allow the new assistant professors to develop the high-quality teaching record and research scholarship record necessary for promotion to associate professor with tenure. We use the following strategies:

- Establishment of clear expectations for performance, with constructive feedback from the Chair of the Cyber Science Department at least twice annually.
- A competitive pay schedule, which includes many step increases within the main categories (assistant professor, associate professor, and professor).
- A travel budget to support conference presentations and attendance.
- Where possible flexibility regarding academic scheduling, so that faculty have some input into the courses that they will be teaching.
- An active mentoring program for all new faculty members.

- Strong encouragement by the Chair of the Cyber Science Department to take full advantage of leave time, in support of a proper work-life balance, with little or no requirements on weekends and holidays.
- Support of sabbaticals for qualified faculty.

E. Support of Faculty Professional Development

Describe the adequacy of support for faculty professional development, how such activities such as sabbaticals, travel, workshops, seminars, etc., are planned and supported.

Faculty professional development is accomplished via several activities. The Naval Academy has a sabbatical program. Sabbaticals can be requested once every seven years and can be requested for either one semester or for one full academic year. It is rare that a sabbatical is denied. On occasion, when the number of requests in one year is unusually high, some faculty members may be encouraged to delay the request to subsequent years. Full salary and benefits are covered for one semester sabbaticals while 70% of salary and benefits are covered for a 10-month period for full academic year sabbaticals.

The CCSS has sufficient funds provided through their annual Expense Budget to support faculty travel to conferences and training courses; this funding is provided to faculty from all units who teach in the program, including Cyber Science, Computer Science, Electrical and Computer Engineering and Systems Engineering. Junior faculty members receive priority treatment, especially with respect to conference travel.

Through the Naval Academy Research Committee, the Academy provides funding, when not otherwise available to junior faculty, to cover their summer salary for their first three years. The Naval Academy also has matched funds to assist in support of faculty members who have partial summer support from external sources.

Faculty members at the Naval Academy are paid for ten months each academic year rather than the more-typical nine months of support at other institutions. The Office of Teaching and Learning at the Naval Academy hosts several teaching workshops on campus after classes are finished and prior to the summer inter-sessional period and also during the winter break. There is no cost to faculty members or programs for attending these workshops, and faculty members are encouraged to attend. In scheduling of faculty teaching schedules, the program strives to provide one day each week free of classes so that faculty members have the opportunity to focus on their research and to develop and participate in research collaborations with nearby research facilities such as the Naval Research Laboratory.

In summary, there is strong support for faculty professional development. We have a strong sabbatical program; travel is well supported; there are ample opportunities to attend workshops and seminars.

PROGRAM CRITERIA

Describe how the program satisfies any applicable program criteria. If already covered elsewhere in the self-study report, provide appropriate references.

As noted in the Criterion 3 discussion, required Outcomes 6 and 7 from the Cybersecurity Program Criteria are now included in the program outcomes. The discussion for Criteria 3 and 4 cover how these outcomes are enabled and how they are assessed.

Regarding Program Criterion 5, we have the following:

At least 45 semester (or equivalent) credit hours of computing and cybersecurity course work.

The following table reflects the number of credit hours of each computing and/or cybersecurity course, reflecting a total of **53** credit hours:

Number	Title	Credits
SY 110	Cyber Security I	3
SY 201	Cyber Fundamentals I	4
SY 202	Cyber Systems Engineering	3
SY 204	Systems Programming/OS Fundamentals	4
SY 301	Data Structures for Cyber Operations	4
SY 303	Applied Cyber Systems Architecture	4
SY 304	Info Operations, Social Engineering & Hacktivism	3
SY 306	Web & Database Cyber Operations	3
SY 308	Security: Fundamental Principles	3
SY 310	Networking & Mobile Computing	4
SY 401	Cyber Operations I	3
SY 402	Cyber Operations II	3
SY 403	Cyber Planning and Policy	3
SY 406	Cyber Law and Ethics	3
SY 4XX	Cyber Elective I	3
SY 4YY	Cyber Elective II	3
Total		**53**

Application of the crosscutting concepts of confidentiality, integrity, availability, risk and adversarial thinking.

While all of these concepts are explored at length in almost all of our courses in one way or another, our introductory course (SY110) is built on the introduction of these concepts and on their application in all areas of cybersecurity. This can be easily seen by reviewing lectures, homework assignments and exams from the SY110 course materials. At the time of the visit, we will provide a digital interface to samples of the introduction and application of these concepts.

Data Security: Protection of data at rest and in transit.

The following **data security** topics are taken directly from the course syllabi and lectures of our various courses:

1. SY110:
    a. Symmetric and asymmetric encryption
    b. Hashing and passwords
    c. Digital cryptography tools and applications
    d. Digital certificates
    e. Steganography
2. SY201:
    a. Hash functions
    b. Password generation/checking
3. SY301:
    a. Public key cryptography
    b. Diffie-Hellman key exchange
    c. Hash tables
    d. Rainbow tables
4. SY306:
    a. Application-level security measures to prevent unauthorized access to data.
    b. Database security
5. SY308:
    a. Pseudo-random functions
    b. Symmetric key encryption
    c. Mode of operations
    d. Message authentication codes
    e. Cryptographic hash functions
    f. Public key encryption
    g. Digital signatures
    h. PKI
    i. Cryptography pitfalls
    j. TLS
6. SY401:
    a. Password cracking using rainbow tables
    b. Pass the hash (cryptanalysis) to authenticate to a remote server using the underlying NT LAN Manager (NTLM) of a user's password, instead of requiring the associating plaintext password.

Software Security: Development and use of software that reliably preserves the security properties of the information and systems they protect.

The following **software security** topics are taken directly from the course syllabi and lectures of our various courses:

1. SY110:
    a. Input validation
    b. Injection attacks

    c. Cross-site scripting
2. SY306:
    a. Attack and defense of Web-based applications
    b. Cross site request forgery attacks
    c. Cross site scripting attacks
    d. SQL injections
3. SY308:
    a. Buffer overflow attacks and countermeasures
    b. Input validation and writing safe program code
4. SY401:
    a. Buffer Overflow – overrun the buffer's boundary and overwrite adjacent memory locations to acquire access.
    b. Web application scanning and exploitation – Front end and backend vulnerability identification and exploitation
    c. Browser Exploitation Framework (BeEF) - Penetration testing tool for web browsers)
    d. Developing exploits
    e. Developing and deploying malware (payloads) with Meterpreter

System Security: Establishing and maintaining the security properties of systems, including those of interconnected components.

The following **system security** topics are taken directly from the course syllabi and lectures of our various courses:

1. SY202:
    a. Vulnerabilities of SCADA systems, industrial control systems and cyber-control systems
2. SY204:
    a. Operating system security and vulnerabilities
3. SY303:
    a. Hardware and software vulnerabilities within the context of a system
4. SY308:
    a. Least privilege, defense-in-depth, vigilance, isolation, input validation, weakest link property
    b. Authentication – passwords and biometrics
5. SY310:
    a. Network security and exploitation
    b. Man-in-the-middle attacks
    c. Amplification Attacks (DNS, Smurf, etc.)
    d. Physical Layer Security (spread spectrum, high-gain antennas, etc.)
6. SY402:
    a. Network monitoring tools
    b. Passive network tools
    c. Detecting Attacks – Snort
    d. Detecting Attacks – Capturing Traffic
    e. Detecting Attacks – Monitoring Traffic
    f. Detecting Attacks – OSSEC

Human Security: Protecting individuals' personal data and privacy; threat mitigation combined with the study of human behavior as it relates to cybersecurity.

The following **human security** topics are taken directly from the course syllabi and lectures of our various courses:

1. SY304:
    a. Social engineering
    b. Psychological underpinnings of online behavior
    c. Hacktivism
2. SY401:
    f. Offensive Cyber Operations planning – applying initial access techniques against the human element.
    g. Applying the Social Engineering Toolkit (SET) – perform advanced, targeted and focused attacks against the human element
3. SY406:
    a. Constitutional foundations of cyber operations/civil liberties
    b. Cybersecurity ethics

Organizational Security: Protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission.

The following **organizational security** topics are taken directly from the course syllabi and lectures of our various courses:

1. SY 402:
    a. Network monitoring
    b. Detecting attacks
    c. Data visualization
    d. Risk management – Vulnerabilities and Actors
    e. Risk management – Calculating Risk
    f. Risk management – Mitigating Risk
    g. Risk assessment lab
    h. Risk analysis – Procurement

Societal Security: Aspects of cybersecurity that can broadly impact society as a whole for better or for worse.

The following **societal security** topics are taken directly from the course syllabi and lectures of our various courses:

1. SY403:
    a. Types and levels of cyber-power threats to national security
    b. US Users of cyber power to achieve success in military and other operations
    c. Linkages between different types/levels of cyber threats and US national and international interests and responses
    d. Foundational US policies and legal considerations, as they relate to both national and international cyber activities
    e. Public policy issues and how they affect the application of cyber power

f. Application of basic concepts of conflict and warfare as they relate to cyber power
g. US Government organization for offensive and defensive cyber power, focusing on DoD.
h. Options for mitigating the vulnerabilities and exploiting the benefits of cyberspace in the face of threats.

2. SY406:
    a. Constitutional foundations of government cyber operations
    b. Constitutional civil liberties that impact military, intelligence and civilian agency cyber operations.
    c. Federal statutes that limit government cyber operations
    d. The structure of US government cyber operations
    e. The laws of war that impact cyber operations
    f. Public-private cybersecurity partnerships
    g. Cybersecurity law for the private sector
    h. Ethical issues that arise with cyber operations.

Advanced cybersecurity topics that build on crosscutting concepts and fundamental topics to provide depth.

We would generally argue that coverage of topics in most 300 and 400-level courses is at the advanced levels. Rather than structuring a detailed argument for all such courses, however, we focus strictly on SY401 and SY402. SY401 is designed to build on previous fundamentals to develop an approach to *offensive* cyber operations, while SY402 is designed to build on previous fundamentals to develop an approach to *defensive* cyber operations. Both courses weave fundamentals into an overall framework of conducting cyber operations within a large-scale, realistic environment – with realistic constraints and assumptions. These courses also involve implementation of a comprehensive capstone project that integrates concepts from previous courses as well – however, both the capstone project *and* the normal syllabus topics build on crosscutting concepts and fundamental topics to provide depth. The topics from SY401 and SY402 are covered in the syllabi provided.

At least 6 semester (or equivalent) credit hours of mathematics that must include discrete mathematics and statistics.

Our program requires 16 hours of mathematics, including Calculus I, II and III and SM242, which includes both discrete mathematics and statistics.

At least one full-time faculty member must hold a doctoral degree in a field related to cybersecurity.

Several of our faculty have doctoral degrees in computer science; some of the faculty also did graduate work specifically in cyber security. Professor Mayberry, for example, has a doctoral degree in computer science and did his dissertation research in cryptography.

APPENDICES

APPENDIX A – COURSE SYLLABI

Course syllabi for the following courses are included here:

1. SY201 — Cyber Fundamentals I
2. SY202 — Cyber Systems Engineering
3. SY204 — Systems Programming and OS Fundamentals
4. SY301 — Data Structures for Cyber Operations
5. SY303 — Applied Cyber Systems Architecture
6. SY304 —Information Operations, Social Engineering, and Hacktivism
7. SY306 — Web and Database Cyber Operations
8. SY308 — Security: Fundamental Principles
9. SY310 — Introduction to Networking and Wireless Communications
10. SY401 — Cyber Operations I
11. SY403 — Cyber Planning and Policy
12. SY402 — Cyber Operations II
13. SY406 — Cyber Law and Ethics

SY 201 – Fundamentals of Cyber Operations I

Course Number / Name	SY201 / Fundamentals of Cyber Operations I
Credits – Contact Hours	4 – 5
Coordinator's Name	Prof. Rose Shumba
Text Book, Title, Author, Year	*Introduction to Programming Using Python*. Y. Daniel Liang, First Ed. Pearson, 2013.
Brief Description of the Content of the Course	This course will teach students problem solving skills in cyber-operations domain using the Python programming language on a Linux platform. Students will analyze the current cyber warfare threats and problems, and code Python programs to solve some of these and related problems.
Prerequisites	None
Required or Elective	Required
Course Goals	• Describe the aspects of the cyber domain and associated security models (supports Discipline Indicators: data security, system security, integrity); • Determine the basic programming concepts required to solve a problem through programming (supports Discipline Indicators: programming, data structures, design, algorithms); • Design, develop, debug, and document programs in Python using structured programming techniques (supports Discipline Indicators: programming, design, implementation, written communications); • Perform normal user operations from the shell in a UNIX environment (supports Discipline Indicators: systems); • Discuss the ethical and professional responsibilities of professionals associated with the cyber domain (supports Discipline Indicators: ethical principles); • Display basic technical communication capabilities (supports Discipline Indicators: verbal communications, written communications); • Describe the importance of and common mechanisms for continuing professional development.

List of Topics Covered	• Cyber Domain Basics:
	  ○ Cyber Operations Introduction
	  ○ Cyber Domain Introduction
	  ○ Cyber Defense Principles
	  ○ Threat Actors
	• Programming Introduction:
	  ○ Programming languages
	  ○ Problem solving in programming
	  ○ Development environment
	  ○ Programming Introduction Lab: Setup VM
	  ○ Programming Introduction Lab: Shell Familiarization
	  ○ Binary, Octal and Hexadecimal number systems
	• Programming Fundamentals
	  ○ Python – Variables
	  ○ Python – Input/Output
	  ○ Python – Arithmetic Operators
	  ○ Python – Conditionals
	  ○ Python – Nested Conditionals
	  ○ Programming Fundamentals Lab: Port Mapper
	  ○ Python – Loops
	  ○ Python – Nested Loops
	  ○ Programming Fundamentals Lab: Stretching
	• Basic reusability:
	  ○ Python – Functions
	  ○ Python – Objects and Methods w/Strings
	  ○ Basic reusability lab – Crack a password

	○ Python – Lists ○ Basic reusability Lab: (Lists) ○ Python – Dictionaries ○ Basic Reusability Lab: (Dictionaries) ○ Recursion ○ Basic Reusability Lab: (Recursion) ○ Python – Classes ○ Basic Reusability Lab: (Classes) • Intermediate Input/Output: ○ Python – Command Line Arguments ○ Intermediate Input/Output Lab: (Command Line Arguments) ○ Python – File I/O ○ Intermediate Input/Output Lab: (File I/O) ○ Python – Sockets ○ Intermediate Input/Output Lab: (Sockets) • Profession: ○ Technical Writing ○ Oral Presentations ○ Continuing Education ○ Professional Ethics

SY 202 – Cyber Systems Engineering

Credits – Contact Hours	3 – 4
Coordinator's Name	Prof. Erick Rodriguez-Seda
Text Book, Title, Author, Year	None
Brief Description of the Content of the Course	An introductory practicum that emphasizes interconnected cyber-physical systems, communications between those systems, the controls and the associated space in which these relationships exist. The student will demonstrate that cyberspace is a domain within the information and electromagnetic environment consisting of the interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and control systems. The theme of this course is for the student to understand that entire communication cycle as it pertains to the cyber physical and communications controls systems.
Prerequisites	SY201 – Cyber Fundamentals I, SM223 – Calculus III, SP211– General Physics
Required or Elective	Required

Course Goals	• Understand tools and techniques used in the design and analysis of cyber-controlled engineering systems
	• Understand and differentiate the notion of open and closed-loop control
	• Apply linear modelling techniques to model simple control systems and predict system response
	• Synthesize a simple control system using a microcontroller, actuators, and sensors
	• Understand and synthesize analog, digital, and serial peripherals as part of a simple embedded system
	• Design, implement, and evaluate a linear control system in a microcontroller to regulate a physical process, while meeting some specific performance criteria
	• Understand the topology, actions, and cyber vulnerabilities—as well as the impact of malicious attacks—within a supervisory control and data acquisition (SCADA) system
	• Basic knowledge on the use of wireless communication and how to affect a cyber-physical system
	• Have a basic knowledge of and familiarity with:
	  ○ MATLAB dynamic simulation capabilities, including SIMULINK
	  ○ C programming language
	  ○ Microcontroller hardware, firmware, and software
	  ○ Serial communication
	  ○ Power supplies
	  ○ Analog, digital, and serial sensors

List of Topics Covered	• Cyber Systems Introduction (Cyber Space, Microprocessors and Control Systems) • Functional Block Diagrams • Electro-Mechanical Translational and Rotational Systems • Transfer Functions • System Time Response • Embedded Systems and mbed microprocessor • Actuators and Sensors • Feedback Control • Serial Communication • Bitwise Manipulation • SCADA Systems, Industrial Control Systems, and Vulnerabilities of Cyber-Control Systems

SY 204 – Systems Programming and Operating Systems Fundamentals

Credits – Contact Hours	4 – 5
Coordinator's Name	LCDR Chris Hoffmeister
Text Book, Title, Author, Year	Kerrisk, Michael. The Linux Programming Interface: A Linux and UNIX System Programming Handbook. No Starch Press, 2010 Prinz, Peter, Kirch-Prinz, Ulla. C Pocket Reference. O'Reilly Media, 2002. Robbins, Arnold. bash Pocket Reference. O'Reilly Media, 2010.
Brief Description of the Content of the Course	In SY204 students expand their programming expertise through the exploration of systems level programming utilizing C. Additionally, students learn the fundamental features and design of operating systems. The activities in the course are covered from a cyber operations perspective. SY204 includes discussions and student activities on cyber operations, students learn about and perform various offensive and defensive techniques throughout the course; the ethical use of computers and information systems is emphasized.
Prerequisites	SY201 or IC210 or SI204
Required or Elective	Required
Course Goals	• Describe computing environment foundational concepts with respect to security from the perspective of the operating system (supports Discipline Indicators: systems, data security, system security, confidentiality, integrity); • Design, develop, debug, and document systems level programs in C using structured programming techniques (supports Discipline Indicators: programming, design, implementation, software security, written communications); • Develop programs to execute in a UNIX environment (supports Discipline Indicators: programming, systems); and • Develop programs that utilize inter process communication (supports Discipline Indicators: programming, systems); and • Design, develop, debug, and document a comprehensive program in a small team (supports Discipline Indicators: programming, design, implementation, written communications, team dynamics); and • Apply principles of secure cyber design to programs used for cyber operations; i.e. design and develop with the adversary in mind (supports Discipline Indicators: data security, software security, system security, confidentiality, integrity, adversarial thinking, offensive cyber operations).

List of Topics Covered	SY204 is organized into six sections: Basic C Programming, Systems Programming Fundamentals, File Systems, Processes, Inter-Process Communication, and Advanced Systems Programming; each of the sections has topics with learning objectives.
	• Basic C Programming:
	  ○ Introduction to C, C Programs, C Variables, C Functions and C Pointers, C Arrays and C Strings, C Comparisons and C Conditionals, C Loops, Preprocessor Directives, Basic C Programming Lab: Password Complexity, Program Analysis (in development for AY2018 Spring offering)
	• Systems Programming Fundamentals:
	  ○ Security Fundamentals, Operating System Overview, Systems Programming Concepts, Descriptor Input/Output (I/O), Systems Programming Fundamentals Lab: Echo the Cat
	• File Systems:
	  ○ Operating System Internals, File Systems – On Disk, File Systems Lab: Hiding from ls, File Systems – Attributes, File

	Systems Lab: Untouchables, File Systems – Access Control Lists, File Systems Lab: Sharing is Good
	• Processes:
	  ○ Process Lifecycle, Process Memory, Dynamic Memory, Signals, Signal Handling, Processes Lab: Baseball, Creating Processes, Monitoring Child Processes, Program Execution, Processes Lab: myShell
	• Inter-Process Communication:
	  ○ I/O Duplication, Pipes, Inter-Process Communication Lab: myShell++, Sockets – Introduction, Sockets – TCP/IP Fundamentals, Sockets – Internet Domain, Inter-Process Communication Lab: netKitty
	• Advanced Systems Programming (possible future offering):
	  ○ Alternative I/O Models, Pseudoterminals

SY 301 – Data Structures for Cyber Operations

Credits – Contact Hours	4 – 5
Coordinator's Name	Prof. Travis Mayberry
Text Book, Title, Author, Year	None
Brief Description of the Content of the Course	In SY301, students learn how to analyze algorithmic runtime and space requirements by learning the tradeoffs of the many different options for how data is stored in a computer. Labs and projects require students to make decisions between the different options, and then apply them to cybersecurity problems, reinforcing the necessity of these general computer science concepts to their chosen discipline. These projects and labs also require students to greatly improve their programming skills.
Prerequisites	SY204
Required or Elective	Required
Course Goals	• Be able to perform complex programming tasks. • Understand the fundamentals of algorithm analysis. • Recognize and apply the canonical ADTs (Lists, Queues, Stacks, Trees, Priority Queues, Maps, and Graphs) appropriate for solving a problem. • Demonstrate the ability to implement the canonical ADTs with arrays, linked lists, binary trees, hash tables, balanced trees, and other similar structures. • Be proficient in defining and coding recursive algorithms, including recognizing when recursive solutions are appropriate. • Understand the role of algorithmic complexity and data structure choices in the cybersecurity domain, and understand the ramifications of data structure and algorithmic choices.
List of Topics Covered	• Big-O Notation • Recursion • Linked Lists • Lists • Stacks • Queues • Trees (self-balancing and otherwise) • Maps and Sets • Hashtables • Priority Queues and Heaps • Rainbow Tables • Graphs • Graph search • Sorting • Complexity and public-key cryptography • Diffie-Hellman key exchange

SY 303 – Applied Cyber Systems Architecture

Credits – Contact Hours	4 – 5
Coordinator's Name	Prof. Dane Brown
Text Book, Title, Author, Year	*The Elements of Computing Systems: Building a Modern Computer from First Principles*, Noam Nisan and Shimon Schocken, MIT Press, 2008.
Brief Description of the Content of the Course	A simple yet functional computer will be designed and implemented using NAND gates and D Flip-Flops. In this project-oriented course, groups will collaborate on each component of this modular system design. A hardware description language will be used to describe the sequential and combinational logic needed to implement each module. The computer will then be prepared to execute high-level object-oriented programs through the designs of an assembler, a virtual machine, and a compiler. Finally, a basic operating system will be designed to allow easy interfacing with the underlying hardware. As time permits, a final project will address a security concern in the overall system or utilize the system to implement an existing security algorithm.
Prerequisites	SY204
Required or Elective	Required
Course Goals	• Understand the relationship between primitive digital logic gates and higher level computer components such as the arithmetic and logic unit and the central processing unit. • Understand the basic architecture of a central processing unit. • Understand the relationship between machine executable instructions, assembly language, and the hardware architecture. • Understand the virtual machine interface and stack operations. • Understand and implement a higher level language and operating system. • Understand and security vulnerabilities at all levels of computing design.
List of Topics Covered	• Boolean Logic • Boolean Arithmetic • Sequential Logic • Machine Language • Computer Architecture • Assembly • Virtual Machine and Intermediate Language • Compiler and High Level Language • Operating Systems

SY 304 – Hactivism and Information Operations in Cyberspace

Credits – Contact Hours	3 – 3
Coordinator's Name	LT Augustine Marinelli
Text Book, Title, Author, Year	• Aiken, Mary. *The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online*, New York: Spiegal & Grau, 2016. • Hadnagy, Christopher, *Social Engineering: The Art of Human Hacking*, Indianapolis: Wiley Publishing, Inc., 2011. • Hoffer, Eric, *The True Believer: Thoughts on the Nature of Mass Movements,* New York: Harper and Brothers, 1951.
Brief Description of the Content of the Course	The "human factor" and the role of individuals and groups in cyber operations is examined with a focus on the use of social-engineering techniques and non-standard approaches used to gain an advantage (technologically, militarily, economically, and intellectually) in the cyber domain. In this context social engineering is the art of exploiting human psychology to gain access to buildings, systems, or data, etc.; it is evolving such that technology solutions, security policies, and operational procedures alone cannot protect resources. In many cases individuals prove to be the largest vulnerability in a network and cyber practitioners need to understand how to defend against or exploit such vulnerabilities. The course examines the following: • Concept of social engineering • How it is done at the person-to-person "tactical" level • The psychological underpinnings of social engineering and online behavior • How nation-states and criminals utilize social engineering within and outside the cyber domain • Analyzes hacktivist groups and other groups operating in the cyber domain through the lenses of mass movement theory • Looks at the overlap and ethics of social engineering and human intelligence
Prerequisites	None
Required or Elective	Required
Course Goals	• Evaluate the group dynamics at work in hacktivist organizations as follows: • Apply mass movement theory and psychology to hacktivist organizations: • Explain the nebulous nature of hacktivist groups; they can be centralized organizations, decentralized organizations, criminal organizations, working on behalf of a nation-state, or some combination of all the above. • Demonstrate understanding of basic social engineering tactics utilized by hacktivist groups in person and in the cyber realm: • Demonstrate effective written and oral communication skills
List of Topics Covered	• Mass Movement and Non-State Actor Theory • Overview of Hacktivists, Criminals, and Nation States in Cyberspace • Social Engineering Tactics, Techniques, and Procedures • Case Studies: Government/Military, State on State • Case Studies: Industrial espionage • Case Studies: Social organizations • Case Studies: Criminal Organizations vs Criminal Organizations

SY 306 – Web and Databases for Cyber Operations

Credits – Contact Hours	3 – 4
Coordinator's Name	Prof. Adina Crainiceanu
Text Book, Title, Author, Year	None
Brief Description of the Content of the Course	The course covers basic web-based application development with a database back-end, with a focus on security. Topics include client side and server side web applications development, the SQL language for relational databases, web authentication, secure web protocols, attack and defense of web-based applications with a database back-end.
Prerequisites	SY301
Required or Elective	Required
Course Goals	• Develop static and interactive client-side web applications. • Query relational databases to satisfy user requirements. • Develop database-backed web applications, for a given database. Implement data access control mechanisms for database security. • Implement application-level security measures to prevent unauthorized access to data. • Understand the principles of common web-based attacks such as cross-site scripting, cross site request forgery, SQL injections
List of Topics Covered	• Introduction to HTML, CSS, and JavaScript • Server-side programming with Python • Web protocols - http, https • Authentication: HTTP Basic authentication, digest, form-based authentication • Cookies, sessions • Relational database model and SQL • Web applications with a database back-end • Database security • Web server configuration • CSRF, XSS attacks • SQL injections

SY 308 – Security Fundamental Principles

Credits – Contact Hours	3 – 3
Coordinator's Name	Prof. Travis Mayberry
Text Book, Title, Author, Year	*Computer Security: Principles and Practice*, 3rd ed. William Stallings and Lawrie Brown. Pearson.
Brief Description of the Content of the Course	This course is an introduction to computer, network and information security. Students will learn the fundamental principles of security while studying various topics including basic cryptography, buffer overflow attacks, and various protocols.
Prerequisites	SY301
Required or Elective	Required
Course Goals	• Explain security fundamental principles such as pillars of cybersecurity, least privilege, defense in-depth, vigilance, isolation, input validation, weakest link property, and Kerckhoff's principle. • List basic cryptographic primitives and explain relevant security definitions. (supports student outcome (i)) • Apply buffer-overflow attacks on simple programs. (supports student outcome (i)) • Analyze a simple information system given the source codes and identify potential vulnerabilities in them. • Use a well-known cryptographic function library such as OpenSSL when writing a software program. • Implement a simple, security-enhanced information system using appropriate cryptographic primitives.
List of Topics Covered	• Cybersecurity Overview • Software Security • Using GDB • Buffer overflow attacks and countermeasures • Input validation and writing safe program code • Cryptography: Pseudorandom functions, symmetric-key encryption, mode of operations, message authentication codes, cryptographic hash functions, public-key encryptions, and digital signatures • PKI • Cryptography pitfalls • Password-based authentication and biometric authentication • TLS • Intrusion detection system • UNIX file access control and setUID

SY 310 – An Introduction to Networking and Wireless Communications

Credits – Contact Hours	3 – 5
Coordinator's Name	MAJ Michael Gardner
Text Book, Title, Author, Year	*Data and Computer Communications*, William Stallings, Tenth Edition, Pearson, 2013
Brief Description of the Content of the Course	An introduction to wired and wireless communications and associated vulnerabilities at the physical, data link and network layers of the TCP/IP model. The theme of this course is for the student to understand the entire communication cycle as it pertains to wired and wireless computer networks and communications systems. Beginning with electromagnetic spectrum and the fundamentals that govern its use, each student will learn the unique implications of operating in a wireless environment. The student will demonstrate applications of interdependent networks, including the Internet and telecommunications networks within the cyberspace domain. Additionally, the student will understand electronics engineering and tactics in support of spectrum dominance and retaining strategic advantage to open and closed networks.
Prerequisites	SY110, SM224, and SP212
Required or Elective	Required
Course Goals	• Describe the fundamental networking technologies and design principles behind internetworking and how these can be exploited by malicious actors. • Discuss steps that should be taken to prevent networks from being exploited and identify who or what is responsible for performing these preventative actions and where or when they should be applied. • Describe, qualitatively and quantitatively, how underlying electromagnetic spectrum technology is implemented in wireless communication and electronic warfare systems. • Evaluate the security and robustness of communications systems by determining which characteristics allow a system to transmit sensitive information to an intended receiver across a noisy or vulnerable channel.
List of Topics Covered	• Communications (Physical Layer Networking): a. Communications Systems Overview b. Signals in time and frequency c. Fourier Analysis d. Bandwidth & Data Rate e. Gain & dB f. Transmission Impairments i. Attenuation, Delay, and Noise g. Signal-to-Noise Ratio h. Channel Capacity i. Transmission Media (Guided & Unguided) j. The Wireless Channel and the Electromagnetic Spectrum k. Propagation i. Modes and Characteristics ii. Line of Sight Transmission iii. Antennas l. Analog & Digital Data m. Analog-to-Digital Conversion n. Signal Encoding i. Digital Data, Digital Signals (Line Coding) o. Digital Data, Analog Signals (Shift Keying) p. Multiplexing & Multiple Access q. Electronic Warfare • Other networking layers: a. Protocol Architecture b. TCP/IP and OSI c. Data Link Layer i. Error Control, Flow Control, Medium Access ii. Error Detection & Correction iii. Ethernet (IEEE 802.3), WiFi (IEEE 802.11)

	d. Network Layer i. IP Addressing 1. Classful IP Addressing 2. Classless Inter Domain Routing 3. IPv4 & IPv6 ii. Address Resolution Protocol iii. Subnets iv. Routing 1. Algorithms and Protocols v. Autonomous Systems vi. Border Gateway Protocol vii. Man-in-the-Middle Attacks e. Transport Layer i. TCP, UDP, Sockets Programming f. Application Layer i. SMTP, DNS, HTTP

SY 401 – Cyber Operations I

Credits – Contact Hours	3 – 4
Coordinator's Name	Prof. Stephen Orr
Text Book, Title, Author, Year	*Essential Cybersecurity Science*, Josiah Dykstra, O'Reilly, 2016.
Brief Description of the Content of the Course	This course will be part I of a two-part course during senior year, during which all aspects of Cyber Operations and course work up to this point will be used to understand project management of a cyber-capstone, cyber policy, and offensive cyber operation methodology.
Prerequisites	SY304 and SY308
Required or Elective	Required
Course Goals	• Understand how Cyber Operations can be a supporting element, a supported element, and an Instrument of National Power. • Understand the phases of an Offensive Cyber Operation (OCO), what each phase entails, and how operations are assessed after completion. • Demonstrate effective communication orally, in writing, and via multimedia. • Create and maintain an effective scholarly research project using best practices. • Access, manipulate, and understand data to aid in effective strategic decision-making. • Identify and evaluate emerging information technologies and their impact on the global environment. • Collaborate in a team environment. • Understand the professional issues and responsibilities in developing a research project for a client. • Have a sound understanding of the tools, techniques, and procedures utilized to exploit information systems and networks. • Possess a thorough understanding of the various types of vulnerabilities (design and/or implementation weaknesses), their underlying causes, their identifying characteristics, and the way in which they are exploited. Know how to take advantage of erroneous implementation of fundamental security design principles. • Be able to identify exploitation vectors and take advantage of them.
List of Topics Covered	• Intro to Cyber Operations • End-to-End Offensive Cyber Operations Methodology • Passive Reconnaissance in an Over-Sharing World • Active Reconnaissance in an Interconnected World • The World Wide Web, Dark Web, Deep Web and a Journey with TOR • Offensive Cyber Operations Planning • Spear Phishing and Water Hole Attacks • Browser Exploitation Framework (BeEF) • Metasploit I • Obfuscation: How Not to Get Caught • Pass the Hash • Exploitation I • Exploitation II • Meterpreter I: Deploying Payloads • Meterpreter II: Advanced Features • Veil Framework and AV Avoidance • Wireless Exploitation and Rogue Access Points • Enumeration • Web Application Scanning • Web Application Exploitation • Attack Payloads • Cyber Operations: An Operator's Perspective

SY 402 – Cyber Operations II

Credits – Contact Hours	3 – 4
Coordinator's Name	LCDR Jeff Kenney
Text Book, Title, Author, Year	None
Brief Description of the Content of the Course	This course will be the second part of a two-part course during senior year, during which all aspects of Cyber Operations and course work up to this point will be used to learn how to adequately defend a network and finalize a Capstone project that is relevant to the Fleet
Prerequisites	SY401
Required or Elective	Required
Course Goals	• Access, manipulate, and understand data to aid in effective strategic decision-making. • Have a sound understanding of the technologies and methods utilized to defend systems and networks. Describe, evaluate, and operate a defensive network architecture employing multiple layers of protection using technologies appropriate to meet mission security goals. • Be able to identify classes of possible threats, what are the consequences associated with each threat, and what actions can be taken to mitigate the threat. • Define, build and present a successful cyber-related capstone
List of Topics Covered	• Virtualization • Networks and Networked Systems • Connecting Networks • Designing the Network Infrastructure • Methods of Securing Systems • Network Monitoring Tools • Passive Network Monitoring • Understanding the Network • Detecting Attacks I (Snort) • Detecting Attacks II (Capturing Traffic) • Detecting Attacks Lab (Monitoring Traffic) • Detecting Attacks III (Using reputation) • Detecting Attacks (Monitoring Traffic II) Lab • Understanding host integrity • Detecting System Attacks I • Detecting System Attacks II with OSSEC • With Data Comes Power • Manipulate Data, Manipulate Minds • Risks of Data • Technology and Data • Risk Management – Vulnerabilities and Actors • Risk Management – Calculating Risk • Risk Management – Mitigating Risk • Risk Assessment Lab • Risk Analysis with respect to procurement - Lab

SY 403 – Cyber Planning and Policy (National Security Decision Making in the Cyber Age)

Credits – Contact Hours	3 – 3
Coordinator's Name	John C. ("Chris") Inglis
Text Book, Title, Author, Year	P. W. Singer and Allan Friedman ("Singer"), Cybersecurity and Cyberwar; (2) Richard A. Clarke and Robert K. Knake ("Clarke"), Cyber War; (3) Benjamin Wittes and Gabriella Blum, The Future of Violence; (4) A compendium of articles and think pieces keyed to topics in the syllabus (typically six to ten articles per lesson).
Brief Description of the Content of the Course	This course is intended to prepare midshipmen to understand the characteristics of all aspects of cyber power and the role of national security decision makers in a world increasingly influenced by cyber power. The course presents students with emerging conceptual, strategic, policy, legal, ethical, organizational, and operational aspects of cyber power, with particular attention to military and naval aspects. However, because that knowledge is and will remain fluid, priority is placed on the development of analytic skills. Thus, what to know about cyber power is combined with how to think about and apply cyber power. Once introduced to key aspects and issues of cyber power, students will be presented with decision-making exercises, simulations, and research tasks to apply and develop such analytic skills. The course covers cyber offensive and defensive challenges across the full range of potential adversaries (criminal, anarchists, and nation-states).
Prerequisites	None
Required or Elective	Required
Course Goals	• Types and levels of cyber-power threats to national security • US uses of cyber power to achieve success in military and other operations • Linkages between different types/levels of cyber threats and US national and international interests and responses • Foundational US policies and legal considerations, as they relate to both national and international cyber activities • Public policy issues and how they affect the application of cyber power • Application of basic concepts of conflict and warfare as they relate to cyber power • US Government organization for offensive and defensive cyber power, focusing on DoD • Options for mitigating the vulnerabilities and exploiting the benefits of cyberspace in the face of threats • How cyber power and conventional military power integrate with one another • Applications of cyber power on Navy/Marine Corps, joint, and coalition operations.
List of Topics Covered	• Cyber Power Fundamentals • Cyber Threats and Vulnerabilities • Cyber Policy and Evolution • US Government Organization and Decision-Making Processes for Cyber • National and International Cyber Norms • Economic Issues and Incentives Related to Cyber • Public Policy Issues in Cyber Space • Tactical Considerations in the Application of Cyber Power • Strategic Considerations in the Application of Cyber Power

SY 406 – Cyber Security Law and Ethics

Credits – Contact Hours	3 – 3
Coordinator's Name	Prof. Jeff Kosseff
Text Book, Title, Author, Year	Court opinions, statutes, regulations, and articles edited by instructor and posted on course website. Supplemented by 30 Lectures of PowerPoint slides
Brief Description of the Content of the Course	This course examines many of the legal and ethical challenges that cyber operations professionals confront in the public and private sectors. The course begins with an in-depth review of the provisions of the United States Constitution that shape the cyber operations of the military and civilian government agencies. The course then reviews the statutes and regulations that provide the government with the authority to conduct cyber operations, as well as the limits that the statutes impose. The course examines the interplay between public-sector and private sector cybersecurity efforts, and the state and federal laws that regulate private-sector cybersecurity. We also explore the ethical considerations that apply to cyber operations
Prerequisites	SY403
Required or Elective	Required
Course Goals	Understand and apply the following concepts: • Constitutional foundations of government cyber operations (Legal Principles, Make Judgments) • Constitutional civil liberties that impact military, intelligence, and civilian agency cyber operations (Legal Principles, Make Judgments, Team Dynamics) • Federal statutes that limit government cyber operations (Legal Principles) • The structure of U.S. government cyber operations (Legal Principles, Societal Security, Confidentiality) • The laws of war that impact cyber operations (Legal Principles, Ethical Principles, Societal Security) • Public-private cybersecurity partnerships (Legal Principles, Make Judgments, Societal Security) • Cybersecurity law for the private sector (Legal Principles, Societal Security, Team Dynamics) • Ethical issues that arise with cyber operations (Ethical Principles, Make Judgments, Team Dynamics)
List of Topics Covered	• Constitutional Foundations of Cyber Operations • Laws Affecting Military and Civilian Government Cyber Operations • Structure of U.S. Government Cyber Operations • Law of Cyberwar/International Legal Issues • Private Sector Cyber Operations Law • Public-Private Cybersecurity Partnerships • Cybersecurity Ethics

APPENDIX B – FACULTY VITAE

A complete set of faculty vitae for AY2018 faculty members supporting the program will be provided to the team before the visit. This appendix contains faculty vitae for most of the AY2017 faculty from Tables 6-1 and 6-2 (complete list below). A * indicates faculty members for which vitae were not available for this document.

- Prof. Dane Brown*
- Prof. Adina Crainiceanu
- Prof. Mark Debels*
- LCDR Benjamin Deckert*
- CDR Dan Devos*
- LCDR Joseph Hatfield
- LCDR Chris Hoffmeister
- Prof. Chris Inglis
- LCDR Jeff Kenney
- Prof. Jeff Kosseff
- Prof. Jim Lewis*
- Prof. Martin Libicki
- LT Augustine Marinelli
- Prof. Travis Mayberry
- LCDR Yasmin Odunukwe
- Prof. Stephen Orr*
- Prof. Allen Parrish
- Prof. Erick Rodriguez-Seda
- Prof. John Roth
- LCDR Andrew Slack
- Prof. Rose Shumba
- CAPT (ret) Paul Tortora*

Faculty Vitae
United States Naval Academy

1. Adina N. Crainiceanu

2. Education
    a. Ph.D. in Computer Science, Cornell University, Ithaca, NY, May 2006
    b. M.S. in Computer Science, Cornell University, Ithaca, NY, January 2004
    c. M.S. in Computer Science, University of Bucharest, Bucharest, Romania, July 1999
    d. B.S. in Computer Science, University of Bucharest, Bucharest, Romania, July 1997

3. Academic experience
    a. Associate Professor, tenured, Computer Science Department, United States Naval Academy, Annapolis, MD, August 2014 - present
    b. Assistant Professor, tenure-track, Computer Science Department, United States Naval Academy, Annapolis, MD, December 2005 – August 2014
    c. Research Assistant, Cornell University, Ithaca, NY, 2001 – 2005
    d. Teaching Assistant, Cornell University, Ithaca, NY, Fall 2003

4. Non-academic experience
    a. Research Associate, Laboratory for Analytical Sciences, Raleigh, NC, Fall 2016
    b. Research Intern, IBM Almaden Research Lab, San Jose, CA, Summer 2002
    c. Research Intern, Reliable Network Solutions, Ithaca, NY, Summer 2001
    d. Programmer Analyst, Kepler, Bucharest, Romania, 1996 – 1999
    e. Programmer Analyst, Transiciel, Lyon, France, Summer 1998
    f. Project Manager, Kepler, Bucharest, Romania, Summer 1997

5. Certifications or professional registrations.
    a. GIAC Certified Web Application Defender (GWEB)
    b. GIAC Web Application Penetration Tester (GWAPT)

6. Current membership in professional organizations
    a. Association of Computing Machinery
    b. Upsilon Pi Epsilon (UPE).

7. Honors and awards
    a. Class of 1951 Faculty Research Excellence Award nominee, Computer Science Department, USNA, 2013
    b. Apgar Teaching Award nominee, Computer Science Department, USNA, 2012

8. Service activities (within and outside of the institution)

Service to Computer Science Department

- Search Committee member: 2010-present
- Curriculum Committee member: 2006-present
- Assessment Committee member: 2006 - present
- Graduate Education Advisor: 2009-2011
- Upsilon Pi Epsilon Faculty Advisor: 2006-2011

- Nimitz Library Liaison: 2006-2011
- Maintain the department level SOF (Student Opinion Forms) database application used each semester for all courses offered by the Computer Science Department, to capture the student opinions. 2006 -2016
- STEM Coordinator: 2009-present
- New Faculty Mentor: LT Keith Labbe AY2010, Capt Pedro Ortiz AY2011, Asst. Prof. Nate Chambers AY2012
- Academic Adviser for SIT and/or SCS majors: 2006-present
- Senior Academic Advisor, SIT and SCS majors. 2011 - present

Service to USNA - Yard-Wide (Campus-Wide)

- Plebe adviser: 2016-present
- Member, Truman Scholarship Committee (2011 - 2014)
- McMullen Fellowship Advisor: Advised interested 1/C and 2/C midshipmen about the McMullen fellowship at University of Pennsylvania.
- USNA STEM-Camps, 2009-present

Service to Professional Community

- Invited panelist for the Cloud Intelligence – Challenges for Research and Industry panel at the 2nd International Workshop on Cloud Intelligence, co-located with the Very Large Database Conference VLDB 2013

- Session chair for 28th IEEE International Conference on Data Engineering ICDE 2012 Conference (3rd ranked conference in the databases research community)
-
- Program Committee Member for 28th IEEE International Conference on Data Engineering ICDE 2012, demo track
-
- Ph.D. Committee member for doctoral candidate Madhushri Banerjee, University of Maryland Baltimore County. Dissertation title: A Utility-Aware Privacy Preserving Framework For Distributed Data Mining With Worst Case Privacy Guarantee, 2011

- The International Journal on Very Large Data Bases (VLDB Journal)
- IEEE Transactions on Parallel and Distributed Systems reviewer
- ACM Transactions on Database Systems (TODS) reviewer
- IEEE Transactions on Knowledge and Data Engineering (TKDE) reviewer
- Data and Knowledge Engineering (DKE) reviewer

9. Briefly list the most relevant publications
    a. Obesity history and daily patterns of physical activity at age 60-64 years: findings from the MRC National Survey of Health and Development. Rachel Cooper, Lei Huang, Rebecca Hardy, Adina Crainiceanu, Tamara Harris, Jennifer Schrack, Ciprian Crainiceanu, Diana Kuh. Journal of Gerontology: Medical Sciences (2016)
    b. Bloofi: Multidimensional Bloom Filters. Adina Crainiceanu, Daniel Lemire. Information Systems, Volume 54, December 2015, pp. 311-324
    c. SPARQL in the Cloud using Rya. Roshan Punnoose, Adina Crainiceanu, David Rapp. Information Systems, Volume 48, March 2015, pp. 181-195

d. Quantifying the reliability of image replication studies: The image intraclass correlation coefficient (I2C2). Haochang Shou, Ani Eloyan, Seonjoo Lee, Vadim Zipunnikov, Adina Crainiceanu, Mary Beth Nebel, Brian Caffo, Martin Lindquist, Ciprian Crainiceanu. Cognitive, Affective, and Behavioral Neuroscience (Journal), December 2013, Volume 13, Issue 4, pp. 714-724
e. Bloofi: A Hierarchical Bloom Filter Index with Applications to Distributed Data Provenance. Adina Crainiceanu. 2nd International Workshop on Cloud Intelligence (Cloud-I 2013) collocated with the 39th International Conference in Very Large Data Bases VLDB. Riva del Garda, Italy, 2013
f. Rya: A Scalable RDF Triple Store for the Clouds. Roshan Punnoose, Adina Crainiceanu, David Rapp. 1st International Workshop on Cloud Intelligence (Cloud-I 2012) collocated with the 38th International Conference in Very Large Data Bases VLDB. Istanbul, Turkey, 2012
g. Load Balancing and Range Queries in P2P Systems using P-Ring. Adina Crainiceanu, Prakash Linga, Ashwin Machanavajjhala, Johannes Gehrke, Jayavel Shanmugasundaram: Journal ACM Transactions on Internet Technology (TOIT) Volume 10 Issue 4, March 2011, pp. 16:1-16:30

10. Briefly list the most recent professional development activities
    - Rya datastore enhancements for Notice to Mariners Datastore Capabilities and Services.(2016-2018)
    - Efficient Query Algorithms and Database Scalability (2014-2016)
    - Semantic processing of large datasets using Rya (Summer 2013)

Faculty Vitae
United States Naval Academy

1. LCDR Joseph M. Hatfield

2. Education
    a. Ph.D. *Politics and International Studies*, University of Cambridge, Cambridge, England, 2015
    b. M.St. *International Relations*, University of Cambridge, Cambridge, England, 2011
    c. B.A. *Philosophy*, University of Missouri-Kansas City, Kansas City, MO, 2005

3. Academic experience
    a. United States Naval Academy, Assistant Professor, Cyber Science Department, 2016-present
    b. United States Naval Academy, Assistant Professor, Political Science Department, 2015-2016

4. Non-academic experience
    a. United States Navy, Intelligence Officer, 2006-present, full-time active duty
        i. Experience includes an operational tour with Helicopter Squadron Five aboard the aircraft carrier USS EISENHOWER (from 2007-2009), working as an analyst at U.S. Africa Command (from 2009-2012), and leading as a staff officer (N2) for Commander Task Force SIX SEVEN (CTF-67) in Sigonella, Sicily (2012-2015).
        ii. Awarded the Joint Service Achievement Medal for work during the 2011 Libya Crisis, where my analytical products were used to brief senior decision makers in the Department of Defense, the Department of State, and the President of the United States. Also awarded the Defense Meritorious Service Medal, and the Navy Commendation and Achievement Medals (each with Gold Stars in lieu of Second Awards).
        iii. Military service includes significant operational experience providing Information Warfare support to Special Operations.
    b. Statistical Quality Control Analyst, Pearson Government Solutions, 2002-2005
        i. Functioned as a key contractually required member of an independent internal reporting/investigating cell whose central role was to be the liaison between the contractor and the United States Federal Government agencies on all Quality-related matters for the EFAST government project.
        ii. Software auditing experience using languages/tools such as SQL, TOAD, Perl, Access, VEDIT, ENDUSER, Visual Basic, and ORACLE-error summaries.
        iii. Responsible for statistical process control, the use of process metrics to determining the root cause of problems, auditing, sampling plans, document control, project coordination, training, as well as frequent interaction with government agencies such as the Department of Labor, Internal Revenue Service, Social Security Administration, as well as the Pension and Welfare Benefits Administration (PWBA), PBGC and EBSA.
    c. Statistical Quality Control Analyst (Six Sigma Black Belt), Bombardier Aerospace Learjet

i. Applied statistical quality control techniques in an effort to improve manufacturing and business practices, gathering and analyzing defect and process data using programs such as Access, Excel and Minitab, leading and working on Six-Sigma teams, performing system and process audits on suppliers, training other departments in quality related functions, and working with the FAA to initiate changes to the quality systems and procedures that govern current manufacturing and business processes.
ii. Analytical techniques included: internal audits, sampling inspections, sampling plans, experience reading blue-prints, extensive experience with corrective action and supplier relations, extensive experience with Quality Systems and procedures including development and verification to Federal Aviation Administration (FAA) regulatory requirements.

5. Certifications or professional registrations
    a. Six Sigma Black Belt, Bombardier Aerospace Learjet
    b. Blueprint Reading Certified

6. Current membership in professional organizations
    a. British International Studies Association

7. Honors and awards
    a. Alfred Thayer Mahan Award for Literary Achievement, 2014
    b. Rear Admiral Thomas A. Brooks Intelligence Officer of the Year, 2013
    c. Madingley Thesis Prize, University of Cambridge, 2011
    d. U.S. Africa Command Company Grade Officer of the Year, 2011
    e. Certificate of Honors in Philosophy, University of Missouri-Kansas City, 2005

8. Service activities
    a. Political Science departmental Scheduler (2015-2016)
    b. Humanities and Social Sciences Division watch officer (2015-2016)
    c. Information Warfare Community Practicum Instructor (2015-present)
    d. Intelligence Officer Service Assignment (2015-present)
    e. USNA Funeral Service Honors (2015-present)
    f. United Kingdom and International Scholarship Program (UKISP) support officer (2015-present)
    g. Mathematics and Sciences Division watch officer (2016-present)
    h. Cyber Science departmental Financial manager (2016-present)
    i. Cyber Science department Curriculum Committee member (2016-present)
    j. Cyber Science department Research Committee member (2016-present)
    k. Cyber Science department Recruitment Committee member (2016-present)
    l. Cyber Europe Language Proficiency, Regional Expertise, Cultural Awareness (LREC) Officer (2016-present)
    m. Cyber Science Department Library Liaison (2016-present)
    n. Cyber Science Department Coordinator for Midshipmen Group Study Programs (2016-present)

9. Briefly list the most important publications and presentations from the past five years
    a. Hatfield, Joseph. *Forthcoming*. "Social Engineering in Cybersecurity: The Evolution of a Concept." *Computers & Security*. (under peer-review).
    b. Hatfield, Joseph. *Forthcoming*. "Don't Look Down: Walzer, MacIntyre, and the Ethical Foundations of War." *Journal of Military Ethics*. (under peer-review).

c. Hatfield, Joseph. 2017. “An Ethical Defense of Treason by Means of Espionage.” *Intelligence and National Security*, Vol. 32, No. 2, pp. 195-207.
d. Hatfield, Joseph. 2017. “Lactantius,” “Anabaptist Pacifism,” and “Tyrannicide,” in *Wars of Religion: An Encyclopedia of Faith and Conflict*, edited by Timothy Demy and Jeffrey Shaw (ABC-CLIO).
e. Hatfield, Joseph. 2017. “Kant’s Perpetual Peace,” in *Philosophers and War*, edited by Timothy Demy, Eric Patterson, and Jeffrey Shaw (Stone Tower Books).

10. Briefly list the most recent professional development activities
    a. Presentation, *Representation Bias and Political Legitimacy*, International Theory Workshop, London School of Economics, London, England (February 2015).

Faculty Vitae
United States Naval Academy

1. LCDR Chris W. Hoffmeister (J-PMP)

2. Education
    a. M.S. *Computer Science*, Naval Postgraduate School, Monterey, CA, 2007.
    b. M.S. *Defense Technology and Systems*, National University of Singapore, Singapore, 2007.
    c. B.S. *Computer Science*, Texas A&M University, College Station, TX, 2001.

3. Academic Experience
    a. Junior Permanent Military Professor, Master Instructor
    Department of Cyber Science
    United States Naval Academy, Annapolis, MD
    Jan 2015 – Current.
    b. Associate Chair, Department of Cyber Science
    United States Naval Academy, Annapolis, MD
    May 2015 – Jul 2017.
    c. Junior Permanent Military Professor, Master Instructor
    Center for Cyber Security Studies
    United States Naval Academy, Annapolis, MD
    Jan 2014 – Dec 2014.
    d. Junior Permanent Military Professor, Master Instructor
    Department of Computer Science
    United States Naval Academy, Annapolis, MD
    Aug 2011 – Dec 2013.

4. Non-Academic Experience
    a. Naval Officer.
        i. Operations Officer, USS HUÉ CITY (CG 66), Dec 2009 – Jul 2011
        ii. Operations Officer, USS ROBERT G BRADLEY (FFG 49), Apr 2008 – Jul 2009
        iii. Training Officer, Main Propulsion Assistant, Electrical Officer, USS TAYLOR (FFG 50), Nov 2001 – Dec 2004.

5. Certifications
    a. GIAC Certified Forensic Analyst (GCFA), Oct 2016 – Oct 2020.
    b. GIAC Certified Forensic Examiner (GCFE), Oct 2015 – Oct 2019.
    c. GIAC Certified UNIX Security Administrator (GCUX), Nov 2014 – Nov 2018.
    d. GIAC Certified Incident Handler (GCIH), Oct 2013 – Oct 2017.
    e. GIAC Certified Intrusion Analyst (GCIA), Dec 2012 – Dec 2020.
    f. GIAC Web Application Penetration Tester (GWAPT), Nov 2012 – Nov 2020.
    g. Information Systems Security Professional, NSTISSI No 4011.
    h. Senior System Managers, CNSSI No. 4012.
    i. System Administration in Information Systems Security, NSTISSI No. 4013.
    j. Information Systems Security Officer, NSTISSI No. 4014.
    k. Systems Certifiers, NSTISSI No. 4015.
    l. Mathematics of Secure Communications, Naval Postgraduate School.

6. Professional Memberships
    a. Association of Computing Machinery (ACM).
    b. Institute of Electrical and Electronics Engineers (IEEE).
    c. Upsilon Pi Epsilon (UPE).

7. Honors and Awards
    a. SANS Lethal Forensicator from SANS FOR408.

8. Service Activities
    a. Service to Math and Science Division
        i. Senior Watch Officer: Responsible for managing military personnel watch assignments, Apr 2012 – Current.
    b. Service to Computer Science Department
        - Executive Assistant, Aug 2011 – Current.
        - Computer Science Academic Advisor: 10 Students.
        - Information Technology Academic Advisor: 2 Students.
        - Capstone Project Advisor, Aug 2011 – Current.
        - Cyber Defense Exercise Affiliate, Dec 2011 – Current.
        - First Lieutenant: Responsible for tracking building/classroom related maintenance/service issues, Aug 2011 – Current.

9. Recent Publications and Presentations
    a. Hoffmeister, C. *Using a Message Board as a Hands-On Learning Tool for Cyber Security II*. Innovations in Cybersecurity Education Workshop (ICEW), University of Maryland Baltimore County (UMBC), 03 Jun 2016.
    b. Hoffmeister, C. *Using a Message Board as a Hands-On Learning Tool for Cyber Security*. Innovations in Cybersecurity Education Workshop (ICEW), University of Maryland Baltimore County (UMBC), 12 Jun 2015.
    c. Brown, C., Crabbe, F., Doerr, R., Greenlaw, R., Hoffmeister, C., Monroe, J., Needham, D., Phillips, A., Schall, S., Schultz, J., Simon, S., Stahl, D., Standard, S., *Developing and Implementing an Institution-Wide Introductory Cyber-Security Course in Record Time*. in Proceedings of the Association of Computing Machinery Southeast [United States] Conference, 2012.
    d. Brown, C., Crabbe, F., Doerr, R., Greenlaw, R., Hoffmeister, C., Monroe, J., Needham, D., Phillips, A., Schall, S., Schultz, J., Simon, S., Stahl, D., Standard, S., Anatomy, *Dissection, and Mechanics of an Introductory Cyber-Security Class's Curriculum at the United States Naval Academy*. in Proceedings of the ACM SIGCSE Innovation and Technology in Computer Science Education (ITiCSE) Conference, 2012.

Faculty Vitae
United States Naval Academy

1. John C. ("Chris") Inglis

2. Education
    a. Graduate of USAF Squadron Officers School, Air Command and Staff College, and the Air War College (Seminar), Montgomery, AL, 1984–1996
    b. Professional Degree, Computer Science, George Washington University, Washington, DC, 1990
    c. Distinguished Graduate USAF Pilot Training, Williams AFB, AZ, 1978
    d. MS. Mechanical Engineering, Guggenheim Fellow, Columbia University, New York, NY, 1977
    e. MS. Computer Science, Johns Hopkins University, Baltimore, MD, 1984
    f. BS. Engineering Mechanics, Distinguished Graduate, USAF Academy, Colorado Springs, CO, 1976

3. Academic experience
    a. Assistant Professor, USNA, Annapolis, MD, Department of Mechanical Engineering, 1982–85
    b. Visiting Professor, Department of Computer Science and Electrical Engineering, USMA, West Point, NY, 1992
    c. *Robert and Mary M. Looker Distinguished Professor of Cyber Studies,* United States Naval Academy, 2014–

4. Non-academic experience
    - 1976–1985 Active Duty USAF Officer and Pilot
    - 1986–2014 Civil Servant, National Security Agency (SES 1997–2014)
        - 1986–1991 Information Security Analyst and Manager within NSA's Information Systems Security Directorate
        - 1991-1992-1995 Participant in NSA Senior Executive Development Program Management. Staff tours in Directorates of Operations, Information Security, and Plans and Programs
        - 1995–96 Deputy Chief, NSA Office of Policy
        - 1996–97 Senior Operations Officer, National Security Operations Center
        - 1997 Promoted to the Senior Executive Service
        - 1998–2001 Deputy Chief, then Chief, NSA Office of China and Korea
        - 2001–03 NSA Director for Worldwide Analysis and Production
        - 2003–06 Special United States Liaison Officer, US Embassy London
        - 2006–14 NSA Deputy Director, Chief Operating Officer
    - 1985–2006 Air National Guard: Rated as Command Pilot. Commanded at Flight, Squadron, Group and Joint Force Headquarters. Retired as Brigadier General USAFR.

5. Certifications or professional registrations.
    - Current Top Secret Clearance, indoctrinated for Special and Compartmented Intelligence (TS/SCI)

6. Current membership in professional organizations. None.

7. Honors and awards (selected)
    a. 1976 Outstanding USAF Academy Cadet in Engineering Mechanics

b. 1984 Clement's Award as the Outstanding Military Faculty Member, USNA
c. 1992 Department of Army Outstanding Civilian Service Award
d. 2000 Presidential Rank Award for Meritorious Service
e. 2002 NSA Exceptional Civilian Service Award
f. 2004 Presidential Rank Award for Distinguished Service
g. 2009 Presidential Rank Award for Distinguished Service
h. 2009 Distinguished Eagle Scout
i. 2014 Director of National Intelligence Distinguished Service Medal
j. 2014 The President's National Security Medal
k. 1976–2006 Military awards include the Air Force Distinguished Service Medal, Legion of Merit, Navy Commendation Medal, and Air Force Commendation Medal

8. Service activities (selected recent)
    a. Member, US Strategic Command Strategic Advisory Group (SAG) and Chair of Its Intelligence Panel
    b. Trustee, Analytic Services Inc (ANSER), a nonprofit corporation, Alexandria, VA
    c. Director, FedEx Corporation
    d. Member-at-large of the Draper Corporation, Boston, MA
    e. Member, Strategic Advisory Group for Lockheed Space Systems, Denver CO
    f. Strategic Advisor to SECURONIX, a security services company incorporated in California
    g. Strategic Advisor to ORBIS Corporation, McLean VA
    h. Strategic Advisor (venture partner) to PALADIN venture capital, Washington DC
    i. Member, Defense Science Board for two panels: *Cyber Deterrence,* and *Autonomy*

9. Briefly list the most relevant publications
    a. "Making Sense of Cyberspace" in draft for publication in the Stanford Review, winter 2015–16.

10. Briefly list recent professional development activities (selected from 40 over two years)
    a. Guest lecturer on the topic of *Security, Privacy and Transparency* at the University of Pennsylvania Law School, the University of Texas Austin, Stanford University Law School, Stanford University Hoover Institute, the US Military Academy, New York University, Georgetown University Law School (November 2013–June 2014).
    b. Panelist at the Joint CIA – Georgetown Security Conference – *Cyber Security and Intelligence Post-Snowden*, 4 March 2014.
    c. Keynote speaker on *Information Security*, Financial Services Information Sharing and Analysis Center Conference (**FS-ISAC**) , Amelia Island, FL, 5 May 2014.
    d. Keynote speaker, *Dealing with Insider Threat in a Globally Connected World*, Symantec Cyber Security Summit, 5 June 2014, Tysons Corner, VA.
    e. Panelists in a Brookings Institute public debate *on "US Surveillance Authorities Require Fundamental Reform,"* 5 June 2014. Hosted by Ben Wittes.
    f. Graduation speaker for the American Military and American public University baccalaureate graduation, 14 June 2014, Washington, DC.
    g. Invited speaker on *Cyber Trends and Strategies* to the Global Digital Leadership Council at the Washington DC Foreign Policy Institute (in conjunction with Harvard University's Belfer Center) on 23 June 2014.
    h. Keynote speech on *"Strategic leadership —theory and practice"* to the National Defense University's Eisenhower College.
    i. Keynote speech on "*Cyber threat and strategy,"* Billington Conference, Washington, DC, 26 August 2014.

j. Testified before the National Science Foundation on "*Technical methods to protect privacy in bulk collections*," 2 September 2014.
k. Conducted a seminar for international journalists from the World Press Institute on the topic of *"National Security for International Benefit,"* Georgetown University, Washington, DC, 5 September 2014.
l. Panel moderator for "*Maintaining the Cyber Research and Development Edge*" at the INSA/AFCEA Conference.
m. Keynote speech to the DoD's Precision Strike Technology Symposium, *"Cyber Underpinnings and Operational Imperatives,"* Johns Hopkins University Applied Physics Laboratory, 21 October 2014.
n. Keynote speaker at the National Defense Industrial Association (NDIA)'s November seminar on the topic of *"Cyber Threat, Cyber Opportunity,"* Arlington, Virginia. 6 November 2015.
o. Testified before the President's Privacy and Civil Liberties Oversight Board on the topic of *"Achieving security **and** privacy,"* Washington, DC, 12 November 2014.
p. Keynote speaker at the Eisenhower Institute fellowship program, Gettysburg College, Pennsylvania on the topic of *"Ten Years Later: Looking at the Office of the Director of National Intelligence – successes, failures, future."*
q. Panel member and speaker at the Bloomberg Conference on *"Cybersecurity 2015: Beyond the Breach."* Specific talk was *"Braving the New Battlefield: National Security in the Digital Age."*
r. Keynote speaker for January meeting of the National Cybersecurity Center of Excellence (NCCoE) Speaker Series (in partnership with Office of Cyber Development, Maryland Department of Business & Economic Development) *"Security in a Cyber World,"* Gaithersburg, MD, 14 January 2015.
s. Keynote speaker at the SRI's Ninth Annual International Conference on Critical Infrastructure, Arlington, Virginia *"Bolstering Cyber Defenses in an age of Convergence, Speed, and Chaos,"* Rosslyn, Virginia, 16 March 2015.
t. Keynote speaker at RAND forum for Cyber awareness and strategy formulation, Arlington, Virginia, 19 March 2015.
u. Chaired a senior leader exercise between the FBI and US Cyber Command, aimed at exercising their collaboration in a cyber crisis, Chantilly, Virginia (FBI's Cyber Center), 14 April 2015.
v. Keynote address to the annual meeting of the [International] Association for Engineering Accreditation (ABET) on the subject of *"Making the case for Cyber Accreditation,"* Atlanta, Georgia, 24 April 2015.
w. Keynote speaker at the Armed Forces Communications and Electronics Association (Maryland Chapter) scholarship awards ceremony on the topic of *"Cyber and its Mandate for Education,"* 7 May 2015.
x. Keynote speaker at the quarterly meeting of the Association of Former Intelligence Officers on the topic of *"Cyber, Security and Privacy,"* 8 May 2015.
y. Addressed the Chief of Naval Operations' task force on "*Cyber Interdependence,"* Arlington, Virginia, 11 June 2015.
z. Panel member in Key Leader Cyber Security forum on "*Cyber strategies for Government and Private Sector Collaboration"* sponsored by New York University and chaired by the former Secretary of the Navy, Richard Danzig, Washington, DC, 11 June 2015.
aa. Keynote speech at the Atlantic Council on *"Cyber Risk and Government Roles,"* Washington, DC, 17 June 2015.

Faculty Vitae
United States Naval Academy

1. LCDR Jeffrey Kenney

2. Education
    a. MS. *Computational Sciences and Informatics,* George Mason Univ, Fairfax VA, 2015
    b. MS. *Computer Science*, Johns Hopkins University, MD, 2007
    c. BA. *Computer Science,* University of Rochester, 2001

3. Academic experience
    a. 2014– Pre, Junior Permanent Military Professor, US Naval Academy

4. Non-academic experience
    a. 2012 - 2014 - Battle Watch Captain and Data/Networking Project Officer - Fleet Cyber Command / U.S. Tenth Fleet
    b. 2009 - 2012 - Cyber Effects Department Head and Global Signals Analysis Laboratory Program Manager – Navy Cyber Warfare Development Group
    c. 2007 - 2009 - Information Warfare Officer - USS BULKELEY (DDG84)
    d. 2003- 2007 - N5 Department Head and NSA Program Manager - Navy Information Operations Command Maryland
    e. 2001 - 2003 - Surface Warfare Officer (Electrical and Communications Officers) - USS VICKSBURG (CG69)

5. Certifications or professional registrations
    a. Information Warfare Officer, Qualified
    b. Surface Warfare Officer, Qualified

6. Current membership in professional organizations
    a. None

7. Honors and awards
    a. Defense Meritorious Service Medal
    b. Meritorious Service Medal
    c. Navy and Marine Corps Commendation Medal (2 awards)
    d. Navy and Marine Corps Achievement Medal (3 awards)
    e. Various Unit and Campaign Medals

8. Service activities (within and outside of the institution)
    a. Officer Representative, Information Warfare Group

9. Briefly list the most relevant publications
    a. None

10. Briefly list the most recent professional development activities
    a. SANS SEC505 Securing Windows Active Directory, 2014

Faculty Vitae
United States Naval Academy

1. Prof. Jeffrey Kosseff

2. Education
    a. JD. *Law*, Georgetown University, Washington, DC, 2010
    b. MPP. *Economic Policy*, University of Michigan, Ann Arbor, MI, 2001
    c. BA. *Economics*, University of Michigan, Ann Arbor, MI, 2000

3. Academic experience
    a. United States Naval Academy, Assistant Professor, Cyber Science Department, 2015-present
    b. American University, Adjunct Instructor, Master in Media Entrepreneurship Program (Communications Law class) 2014-2015 (part-time adjunct)

4. Non-academic experience
    a. Covington & Burling LLP, Cybersecurity Attorney (Associate), 2012-2015, full-time
    b. United States Court of Appeals for the Ninth Circuit, Law Clerk to Judge Milan D. Smith, Jr., 2011-2012, full-time
    c. United States District Court for the Eastern District of Virginia, Law Clerk to Judge Leonie M. Brinkema, 2010-2011, full-time
    d. The Oregonian, journalist, 2001-2008, full-time

5. Certifications or professional registrations
    a. Certified Information Privacy Professional/US (International Association of Privacy Professionals)
    b. Active member of the District of Columbia bar
    c. Associate member of the Virginia bar

6. Current membership in professional organizations
    a. International Association of Privacy Professionals

7. Honors and awards
    a. Finalist, 2007 Pulitzer Prize for National Reporting
    b. 2006 George Polk Award for National Reporting
    c. Georgetown University Law Center: Magna Cum Laude, Order of the Coif, Top 3% of Graduating Class

8. Service activities
    a. United States Naval Academy, Faculty Senate (2015-present)
    b. International Association of Privacy Professionals, Publications Advisory Board (2014-present)
    c. Media Law Resource Center, Legislative Affairs Committee Co-Chair (2014-2015)

9. Briefly list the most important publications and presentations from the past five years
    a. Cybersecurity Law (textbook/treatise), published by Wiley, February 2017
    b. The Twenty-Six Words that Created the Internet, book about Section 230 of the Communications Decency Act, under contract with Cornell University Press

(detailed outline/proposal accepted in December 2016; full manuscript due January 2018)

c. Defining Cybersecurity Law, Iowa Law Review (accepted for publication in February 2017)
d. Twenty Years of Intermediary Immunity: The U.S. Experience, SCRIPTed: A Journal of Law, Technology & Society (accepted for publication via peer review, to be published in June 2017)
e. The Cybersecurity Privilege, *I/S: A Journal of Law and Policy for the Information Society* (2017)
f. A New Legal Framework for Online Anonymity, *IEEE Security & Privacy* (2015)
g. Cyber-Physical Systems and National Security Concerns, chapter in forthcoming book, *Security and Privacy in Cyber-Physical Systems: Foundations and Applications* (Wiley)
h. Private or Public? Eliminating the Gertz Defamation Test, *University of Illinois Journal of Law, Technology & Policy* (2011)
i. Defending Section 230: The Value of Intermediary Immunity, *Journal of Technology Law and Policy* (2010)
j. Contributor to TechCrunch, Forbes, Privacy Perspectives, and other technology and privacy publications

10. Briefly list the most recent professional development activities
    a. Presentation, *Understanding the Cybersecurity Act of 2015*, BSidesCharm 2017 conference, Baltimore, MD (April 30, 2017)
    b. Presentation, *Cybersecurity and Attorney-Client Privilege: How to Get the Truth While Protecting Your Company*, InfoGovCon, Hartford, CT (Sept. 30, 2015)
    c. Presentation, *Big Data and Privacy by Design*, Big Data TechCon, Boston, MA (April 28, 2015)
    d. Panelist, *Drones and Privacy*, NIST Information Security and Privacy Advisory Board (Oct. 23, 2014)

Faculty Vitae
United States Naval Academy

1. Prof. Martin Libicki

2. Education
    a. PhD, Economics, UC Berkeley, 1978.
    b. M.C.P., City and Regional Planning, UC Berkeley, 1974.
    c. S.B., Mathematics, MIT, 1972.

3. Academic experience
    a. United States Naval Academy, Distinguished Visiting Professor, Cyber Science Department, 2011-present
    b. Columbia University, Adjunct Professor, 2014.
    c. Georgetown University, Adjunct Professor, 2009-2011.

4. Non-academic experience
    a. Senior Management Scientist, RAND Corporation, 1998-2016.
    b. Senior Fellow, Institute for National Strategic Studies, 1986-1998.
    c. Head, US Navy Industrial Preparedness Planning Program, 1982-1986.
    d. Economist, Energy and Minerals Division, US General Accounting Office, 1979-1982.

5. Certifications or professional registrations
    a. None

6. Current membership in professional organizations:
    a. None

7. Honors and awards:
    a. None

8. Service Activities:
    a. None

9. Briefly list the most important publications and presentations from the past five years:
    a. "The Convergence of Information Warfare," *Strategic Studies Quarterly,* forthcoming.
    b. "Second Acts in Cyberspace," *Journal of Cybersecurity*, forthcoming.
    c. "The Cyber War that Wasn't" in Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015.
    d. "Waging Cyber War the American Way" (with David Gompert), *Survival*, (August-September 2015).
    e. "Cyber House Rules: On War, Retaliation, and Escalation," (with David Gompert and Larry Cavaiola), *Survival* (February-March 2015).
    f. "Sino-U.S. Crisis Instability and Cyber-Warfare," (with David Gompert), *Survival* (August-September 2014).
    g. "Is Cyberwar Good for Peace?" http://www.observatoire-fic.com/is-cyberwar-good-for-peace/ (September 2014)
    h. "Dealing with Cyberattacks," in Chrisopher Preble and John Mueller, *A Dangerous World*, Washington DC (Cato Institute), 2014.

i. Why Cyber War Will Not and Should Not Have its Grand Strategist," *Strategic Studies Quarterly* (Spring 2014), pp. 23-39.
j. "The Specter of Non-Obvious Warfare," *Strategic Studies Quarterly* (Fall 2012), pp. 88-101.
k. "Why Cyberspace is not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* (Fall 2012), pp. 325-340.

10. Briefly list the most recent professional development activities:
    a. None

Faculty Vitae

United States Naval Academy

1. LT Augustine Marinelli, United States Navy

2. Education
    a. M.A. Political Science, Villanova University: 2009
    b. B.A. Political Science and Italian Language, Villanova University: 2007

3. Academic experience
    a. Senior Instructor: United States Naval Academy: June 2014–Present
        i. Center for Cyber Security Studies
            1. Taught cyber operations courses and other subjects within the discipline
    b. Research Assistant: Villanova University Political Science Dept.: 2007–09
        i. Conducted academic research for faculty in exchange for full tuition scholarship
        ii. Substitute-taught class and proctored exams

4. Non-Academic experience
    a. United States Navy Officer: 2009–Present
        i. Explosive Ordnance Disposal Mobile Unit 12: 2012–14
        ii. Fleet Air Reconnaissance Squadron Two: 2010–12
    b. Research Associate: 2008
        i. Economy League of Greater Philadelphia: June–August 2008

5. Certifications or professional registrations. None.

6. Current membership in professional organizations
    a. Pi Sigma Alpha National Political Science Honor Society

7. Honors and awards
    a. Academic Awards:
        i. Villanova University Fritz Nova Award for Academic Excellence in Political Science (2007)
    b. Non-Academic Awards:
        i. Navy and Marine Corps Commendation Medal
        ii. Navy and Marine Corps Achievement Medal
8. Service activities
    a. Service to U.S. Naval Academy
        i. Funeral Honors Support Detail Officer: June 2014–Present
            1. Led rendering of military honors at official funerals
    b. Service to Center for Cyber Security Studies:
        i. SY304 Course Coordinator: June 2014–Present
            1. Developed, taught, and updated SY304 course of instruction

ii. Curriculum Committee Member: June 2015–Present
iii. Faculty Liaison to Cyber Policy Teams: November 2014–Present
    1. Coordinated logistics, sought legal approval, and provided on-site support to USNA midshipmen competing in academic cyber policy competitions
iv. Leahy Hall First Lieutenant: July 2014–Present
    1. Led effort to ensure timely maintenance and repairs to CCSS office spaces

9. Briefly list the most relevant publications
    a. "Think You Know War Strategy," *Philadelphia Daily News*, March 2008.
    b. "Intelligence and Third-Party Intervention in Unconventional Civil/Sectarian Conflicts: The British in Malaya and American Military in Lebanon," *Small Wars Journal*, 28 March 2009.

10. Briefly list recent professional development activities. None.

Faculty Vitae
United States Naval Academy

1. Prof. Travis Mayberry

2. Education
    a. PhD. *Computer Science*, Northeastern University, Boston, MA, 2015
    b. BS. *Computer Science*, University of Maryland, Baltimore County, Baltimore, MD, 2008

3. Academic experience
    a. Research Assistant, Northeastern University, Boston, MA, 2010-2015
    b. Lecturer, Northeastern University, Boston, MA, 2010-2015
    c. Research Assistant, MIT Lincoln Laboratory, Lexington, MA, 2011-2012

4. Non-academic experience
    a. Software Developer, ImageScan, Lanham, MD, 2007-2010

5. Certifications or professional registrations
    a. None

6. Current membership in professional organizations
    a. International Association for Cryptologic Research
    b. International Financial Cryptography Association

7. Honors and awards
    a. Network and Distributed Systems Security Symposium Distinguished Paper Award, 2014
    b. Northeastern University College of Computer Science and Information Technology Student Research Award, 2014
    c. NSF Scholarship for Service Fellowship, 2012-2014
    d. Northeastern University Dean's Fellowship, 2010

8. Service activities (within and outside of the institution)
    a. Chair of the SCY Research Committee
    b. Program Committee Member, Financial Cryptography
    c. Member of SCY Curriculum Committee, SCY Hiring Committee, and Division II Curriculum Committee

9. Briefly list the most relevant publications
    a. Tarik Moataz, Travis Mayberry, Erik-Oliver Blass: Constant Communication ORAM with Small Blocksize., ACM Computer Communication Security 2015
    b. Erik-Oliver Blass, Travis Mayberry, Guevara Noubir, Kaan Onarlioglu: Toward Robust Hidden Volumes using Write-Only Oblivious RAM, ACM Computer Communication Security 2014
    c. Travis Mayberry, Erik-Oliver Blass, Agnes Hui Chan: Efficient Private File Retrieval by Combining ORAM and PIR., Network and Distributed Systems Security 2014

Faculty Vitae
United States Naval Academy

1. LCDR Yasmin M. Odunukwe

2. Education
    a. M.S. *Engineering Management*, University of Maryland Baltimore County, Catonsville, MD, 2011
    b. B.S. *Mathematics*, United States Naval Academy, Annapolis, MD, 2006

3. Academic experience
    a. United States Naval Academy, Junior Permanent Military Professor, Cyber Science Department, 2016-present

4. Non-academic experience
    a. United States Navy, Cryptologic Warfare Officer, 2006-present, full-time active duty
        i. Experience includes a tour at the National Security Agency (NSA) (2006-2009) serving as an analyst and watch floor officer on the NSA Operations Center, acquisition/project management tour at Navy Cyber Warfare Development Group (2009-2012), operational tour aboard the USS NITZE (2012-2014), and as a staff officer for OPNAV N2/N6F3, Integrated Fires for the Deputy Chief of Naval Operations for Information Dominance.
        ii. Awarded the Joint Service Achievement Medal for work during tour on NSOC, where my analytical products were used to brief senior decision makers in the Department of Defense, the Department of State, and the President of the United States. Also awarded the Navy Commendation Medal (with Gold Stars in lieu of third Awards).

5. Certifications or professional registrations
    a. DAWIA level two certification in Engineering and Program Management Blueprint

6. Current membership in professional organizations
    a. National Naval Officer Association

7. Honors and awards
    a. NSOC Outstanding Military Performer, 2008

8. Service activities
    a. Cyber Science Internship Coordinator (2016-present)
    b. Math and Science Division watch officer (2016-present)
    c. Cyber Science departmental First Lieutenant (2016-present)
    d. Cyber Science department Search Committee member (2016-present)
    e. Cyber Science department Recruitment Committee member (2016-present)

Faculty Vitae
United States Naval Academy

1. Prof. Allen Parrish

2. Education
    a. PhD, *Computer Science*, The Ohio State University, Columbus, OH, 1990.
    b. MS, *Computer Science*, The Ohio State University, Columbus, OH, 1987.
    c. BS. *Computer Science*, The University of Tennessee at Martin, Martin, TN, 1983.

3. Academic experience
    a. Professor and Chair, Department of Cyber Science, US Naval Academy, Annapolis, MD, 2016-Present.
    b. Professor, Associate Professor, Assistant Professor, Department of Computer Science, The University of Alabama, Tuscaloosa, AL, 1990-2016.
    c. Associate Vice President for Research, The University of Alabama, Tuscaloosa, AL, 2015-16.
    d. Founding Director, Center for Advanced Public Safety, The University of Alabama, 2000-2016.

4. Non-academic experience
    a. None

5. Certifications or professional registrations
    a. None

6. Current membership in professional organizations
    a. ACM, IEEE, IEEE-CS, Association of Transportation Safety Information Professionals.

7. Honors and awards
    a. ABET Fellow, 2016.
    b. CSAB Fellow, 2014.
    c. T. Morris Hackney Endowed Faculty Leadership Award, College of Engineering, The University of Alabama, 2012.

8. Service activities (within and outside of the institution)
    a. Computing accreditation activities including:
        i. CSAB Program Evaluator, 1996-2000.
        ii. ABET CAC Team Chair and Commissioner 2001-2012, 2015-present.
        iii. ABET CAC Executive Committee, 2005-2012.
        iv. ABET CAC Vice-Chair for Operations, 2008-2009.
        v. ABET CAC Chair-Elect, 2009-2010
        vi. ABET CAC Chair, 2010-2011.
        vii. ABET CAC Past Chair, 2011-2012.
        viii. CSAB Board of Directors, 2013-present.
        ix. CSAB Secretary-Treasurer, 2015-present.
        x. CSAB Criteria Committee Chair, 2012-present.
        xi. CSAB *Ad Hoc* Committee on Cybersecurity, 2014-present.
        xii. ABET CAC representative to the IEEE Accreditation Policy Council, 2006.

xiii. IEEE Computer Society Accreditation Chair, 2015.

b. Member, Cyber Education Project Steering Committee, 2014-present.
c. Member, ACM Joint Task Force on Cyber Security Curriculum, 2015-present.
d. Member, IEEE Computer Society Professional and Educational Activities Board, 2016-Present, 1994-2004.
e. IEEE Computer Society Accreditation and Curriculum Subcommittee Chair, 2016.
f. ATSIP (Association of Transportation Safety Information Professionals) Board of Directors, 2012-present.

9. Briefly list the most relevant publications
    a. Myers, L., A. Parrish and A. Williams, "Big Data and the Fourth Amendment: Reducing Overreliance on the Objectivity of Predictive Policing," *Federal Courts Law Review,* Volume 8, no. 2, 2015, pp. 231-244.
    b. Greenlaw, R., A. Phillips and A. Parrish, "Is It Time for ABET Criteria in Cybersecurity?," *ACM Inroads*, vol. 5, no. 3, September 2014, pp. 44-48.
    c. Ding, L., Steil, D., Dixon, B., Kraft, N., Brown, D., Parrish, A., "FIRST: A Framework to Integrate Relationship Search Tools," *International Journal of Computers and Applications*, 2013.
    d. Ding, L., Steil, D., Dixon, B., Parrish, A., Brown, D., "A Relation Context Oriented Approach to Identify Strong Ties in Social Networks," *Knowledge Based Systems,* volume 24, no. 8, 2011, pp. 1187-1195.
    e. Steil, D.A., J.R. Pate, N. A. Kraft, R. Smith, B. Dixon, L. Ding, A. Parrish, "Patrol Routing Expression, Execution, Evaluation and Engagement," *IEEE Transactions on Intelligent Transportation Systems,* Vol. 12, No. 1, March 2011.

Faculty Vitae
United States Naval Academy

1. Erick J. Rodríguez-Seda

2. Education
    a. PhD. *Electrical and Computer Engineering*, University of Illinois, Urbana-Champaign, IL, 2011
    b. MS. *Electrical Engineering*, University of Illinois, Urbana-Champaign, IL, 2007
    c. BS. *Electrical Engineering*, University of Puerto Rico, Mayagüez, PR, 2004

3. Academic experience
    a. Assistant Professor, Department of Weapons and Systems Engineering, *United States Naval Academy*, Annapolis, MD, 2013 - Present

4. Non-academic experience
    a. Post-Doctoral Research Associate, Erik Jonsson School of Engineering and Computer Science, University of Texas at Dallas, Richardson, TX, 2011 – 2013
    b. Intern, *The Boeing Company*, Bellevue, WA, Summers 2008, 2009

5. Certifications or professional registrations
    a. None

6. Current membership in professional organizations
    a. None

7. Honors and awards
    a. Best Paper in Session Award, Time Delay Systems Session, American Control Conference, 2010

8. Service activities (within and outside of the institution)
    a. Senior Plebe Adviser, USNA
    b. WSE Department Webmaster, USNA
    c. Systems Outreach Committee, USNA
    d. Robotics Major Committee, USNA
    e. Capstone and Research Mentor Adviser, USNA
    f. Referee for multiple professional journals and conference

9. Briefly list the most relevant publications
    a. E. J. Rodríguez-Seda, D. M. Stipanovic, and M. W. Spong, "Guaranteed Collision Avoidance for Autonomous Systems with Acceleration Constraints and Sensing Uncertainties," Journal of Optimization Theory and Applications, vol. 168, no. 3, pp. 1014-1038, March 2016.
    b. E. J. Rodríguez-Seda, "Passive Transparency Compensation for Bilateral Teleoperators with Communication Delays," Journal of Robotics, vol. 2015, Article ID 861425, 13 pages, 2015.
    c. E. J. Rodríguez-Seda, C. Tang, M. W. Spong, and D. M. Stipanovic, "Trajectory Tracking with Collision Avoidance for Nonholonomic Vehicles with Acceleration Constraints and Limited Sensing," International Journal of Robotics Research, vol. 33, no. 12, pp. 1569-1592, Oct. 2014.

d. E. J. Rodríguez-Seda, D. M. Stipanovic, and M. W. Spong, “Teleoperation of Multi-Agent Systems with Nonuniform Control Input Delays,” Integrated Computer-Aided Engineering, vol. 19, no. 2, pp. 125-136, 2012.
e. E. J. Rodríguez-Seda, J. J. Troy, C. A. Erignac, P. Murray, D. M. Stipanovic, and M. W. Spong, “Bilateral Teleoperation of Multiple Mobile Agents: Coordinated Motion and Collision Avoidance,” IEEE Transactions on Control Systems Technology, vol. 18, no. 4, pp. 984-992, July 2010.
f. E. J. Rodríguez-Seda, D. J. Lee, and M. W. Spong, “Experimental Comparison Study of Control Architectures for Bilateral Teleoperators,” IEEE Transactions on Robotics, vol. 25, no. 6, pp. 1304-1318, Dec. 2009.

10. Briefly list the most recent professional development activities
    a. Attended and participated in the following professional, international conferences:
        a. International Symposium on Resilient Control Systems, 2015
        b. IEEE Int. Conf. on Robotics and Automation, 2015
        c. IEEE/RSJ Int. Conf. on Intelligent Robots and Systems, 2014
        d. American Control Conference, 2014
    b. Participated in a series of webinars on new research trends by the Missouri University of Science and Technology’s Control Systems Forum.

Faculty Vitae
United States Naval Academy

1. John D. Roth

2. Education
    a. Ph.D. *Electrical Engineering,* Naval Postgraduate School, 2016
    b. MS. *Electrical Engineering,* Naval Postgraduate School, 2012
    c. BS. *Electrical Engineering*, U.S. Naval Academy, 2004

3. Academic experience
    a. Assistant Professor, Cyber Science Deparmment
       U.S. Naval Academy
       Jan 2016 - May 2016
    b. Instructor, Department of Electrical and Computer Engineering
       U.S. Naval Academy
       Jan 2013–Dec 2015

4. Non-academic experience
    a. Headquarters Company Commander, Marine Corps Mountain Warfare Training Center
       2008–10
    b. Assistant Logistics Officer, 3d Battalion, 1st Marines
       2005–08

5. Certifications or professional registrations
    a. Fundamentals of Cyber Security – Naval Postgraduate School

6. Current membership in professional organizations
    a. IEEE Student Member

7. Honors and awards
    a. Graduate with Distinction – Naval Postgraduate School, 2012
    b. IEEE/Eta Kappa Nu Award in Engineering Excellence, 2012
    c. Graduate with Merit – U.S. Naval Academy, 2004

8. Service activities (within and outside of the institution)
    a. Bowman Scholar Advisor, AY2016
    b. SY303 Course Coordinator, AY2016
    c. Honor liaison, ECE Department 2013–15

9. Briefly list the most relevant publications
    a. J.D. Roth, M. Tummala, J.C. McEachen, and J.W. Scrofani, "On Location Privacy in LTE," *IEEE Transactions on Information Forensics and*

Security, 2016.

b. J. D. Roth, M. Tummala, and J.C. McEachen, "A Computationally Efficient Approach for Hidden-Markov Model-Augmented Fingerprint-Based Positioning," *International Journal of Systems Science*, 2015.
c. J. D. Roth, M. Tummala, and J.C. McEachen, "A Computationally Efficient Approach for Hidden-Markov Model-Augmented Fingerprint-Based Positioning," *International Journal of Systems Science*, 2015. J. D. Roth, M. Tummala, J. W. Scrofani, "Cellular Synchronization Assisted Refinement (CeSAR): A Method for Accurate Geolocation in LTE-A Networks," in *Proceedings of the Hawaii International Conference on Systems Science*, 2016, to be published.
d. J. D. Roth, M. Tummala, J. C. McEachen, and J. W. Scrofani, "On Mobile Positioning Via Cellular Synchronization Assisted Refinement (CeSAR) in LTE and GSM Networks," in *Proceedings of the International Conference on Signal Processing and Communication Systems*, 2015, to be published.
e. J. D. Roth, M. Tummala, J. McEachen, and J. Scrofani, "Location Estimation via Sparse Signal Reconstruction in Subsampled Overcomplete Dictionaries for Wireless 4G Networks," in *Proceedings of the Hawaii International Conference on Systems Science*, 2015.
f. J. D. Roth, M. Tummala, J. C. McEachen, and J. W. Scrofani, "A k-Generation Approach to Wireless Fingerprinting for Position Estimation," in *Proceedings of the International Conference on Signal Processing and Communication Systems*, 2014.
g. J. D. Roth, M. Tummala, J. McEachen, and J. Scrofani, "A Scalable Hidden-Markov Model Algorithm for Location-Based Services in WiMAX Networks," in *Proceedings of the Hawaii International Conference on Systems Science*, 2014.

10. Briefly list the most recent professional development activities
    a. Effective College Teaching Workshop – 2014
    b. Wireless Symposium at Virginia Tech – 2015
    c. Exploiting Real-Time Operating Systems – 2015

Faculty Vitae
United States Naval Academy

1. Prof. Rose Shumba

2. Education:
   a. PhD Computer Science, University of Birmingham, England, UK, 1995.
   b. MS Computer Science, University of Manchester Victoria, England, UK, 1990.
   c. BS Computer Science and Business Studies, University of Zimbabwe.

3. Academic Experience:
   a. Professor, Cyber Science Department, US Naval Academy, 2016-Present.
   b. Interim Vice Dean, UMUC, Cyber Security and IA Department, 7/2015 – 12/2015.
   c. Associate Vice Dean and Program Chair, UMUC, 2012-2016.
   d. Director NSA IA Center, Indiana University of Pennsylvania, 2008-2012.
   e. Professor, Computer Science Department, Indiana University of Pennsylvania, 2002-2012.
   f. Chair, Computer Science Department, University of Zimbabwe, 1997-2001.

4. Non-Academic Experience:
   a. None

5. Certifications or professional registrations:
   a. None

6. Current membership in professional organizations:
   a. IFIP WG3, ACM SIGCSE, IFIP WG11.9, NIST Cloud Computing WG

7. Honors and Awards:
   a. None

8. Service Activities:
   a. Senior Academic Adviser, 2016-Present.
   b. Faculty Search Committee Chair, 2016-Present.
   c. Curriculum Committee Chair, 2016-Present.

9. Briefly list the most relevant publications:

   Paul Wang, Rose Shumba, William Kelly, "Security by Design: Defense-in-depth IoT Architecture," *Journal of the Colloquium for Information Systems Security Education,* Edition 4, Issue 2, February 2017.

   Elizabeth K Hawthorne, Rose K Shumba, "Teaching Digital Forensics and Cyber Investigations Online: Our Experiences," European Scientific Journal (ESJ) ISSN-1857-7881 (Print) and co-presented at the Annual International Interdisciplinary Conference in Azores, Portugal, July 2014.

Rose Shumba, "Towards a Digital Forensics Competency-Based Program: Making Assessment Count" presented at 10th Annual Association of Digital Forensics Security and Law Conference, May 2015.

Rose Shumba, C. Taylor, et al, "Cyber Security, Women and Minorities – Findings and Recommendations from a Preliminary Investigation," ITiCSE Working Group Report, Proceedings of the 18th Annual Conference on Innovation and Technology in Computer Science Education, Kent, July 1-3, 2013.

Faculty Vitae
United States Naval Academy

1. LCDR Andrew Slack

2. Education
    a. MS. *Computer Science*, Naval Postgraduate School, Monterey, CA, 2009
    b. BS. *General Science,* United States Naval Academy, MD, 2002

3. Academic experience
    a. 2014– Pre, Military Instructor, US Naval Academy

4. Non-academic experience
    a. Aug 2011–March 2014 – Experimentation, Testing, and Integration Department Head, Legal Officer – Navy Cyber Warfare Development Group
    b. 2009–2011 –Ship's Signals Exploitation Space (SSES) Division Officer, Assistant Intelligence Officer, Supplementary Plot (SUPPLOT) Watch Officer, and QUEBEC Module Watch Officer – CVN-76, USS RONALD REAGAN
    c. 2004–2007 – Watch Officer – NSA/CSS Threat Operations Center (NTOC) – NIOC MD

5. Certifications or professional registrations
    a. Information Warfare Officer, Qualified
    b. GIAC Penetration Tester, Qualified

6. Current membership in professional organizations
    a. None

7. Honors and awards
    a. Joint Service Commendation Medal
    b. Navy and Marine Corps Commendation Medal
    c. Navy and Marine Corps Achievement Medal (2 awards)
    d. Various Unit and Campaign Medals

8. Service activities (within and outside of the institution)
    a. Officer Representative, Information Warfare Group

9. Briefly list the most relevant publications
    a. None

10. Briefly list the most recent professional development activities
    a. SANS SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking, 2016
    b. SANS SEC560 Network Penetration Testing and Ethical Hacking, 2015
    c. SANS SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling, 2014

APPENDIX C – EQUIPMENT

Please list the major pieces of equipment used by the program in support of instruction.

Please list the major pieces of equipment used by the program in support of instruction.

All midshipmen are required to purchase a laptop in their plebe year. ITSC works closely with vendors to outfit the laptops with the best technology and software at the most affordable price. The specifications for the Plebe Class of 2020 (incoming freshmen in Fall AY2017) are:

Manufacturer, Model	NCS Technologies with HP EliteBook 840 G3
Processor	Intel 6th Generation Core i7-6600U Processor (2.6GHz, up to 3.4GHz, 4MB cache)
Memory	8GB DDR4 2133 MHz (1x8GB)
Hard Drive	512GB Mobility Solid State Drive
Video	Integrated Intel HD Graphics 520
Display	14-inch HD (1366 x 768), Anti-glare Screen
Wireless	Integrated 802.11 ac/a/b/g/n Dual Band 2x2, 2.4GHz, 5 GHz
NIC	Integrated 100/1000 Gigabit Ethernet Controller
Ports	Two (2) USB3.0 and One (1) USB Type C, One Headphone/Microphone Jack
Smart Card Reader	Integrated Smart Card Reader
TPM	TPM 1.2/2.0
Operating System	Microsoft Windows 10 Professional 64-Bit
Weight	3.50 lbs
Dimensions	Width: 13.3 in / 33.8 Height (rear): 0.74 in / 1.89 cm Depth: 9.3 in / 23.7 cm
Battery Life	3 Cell (46Wh) Battery, Up to 13.5 Hours Battery Life
Warranty	4-year No Fault (Accidental Damage) Parts Warranty with Keep Your Hard Drive Protection. 4-year Battery Warranty

Computer Labs:
While most classes are designed to conduct lab sessions with the student's laptops, some courses are taught in standalone computer labs (such as SY204). These labs consist of desktop computers loaded with the most recent LTS version of Ubuntu and any associated or requested software (such as Atom text editor). Each of these computers are accessible from anywhere on campus via SSH, enabling the students to work on assignments and projects from their room.

Advanced classes (SY401) are using Apple MacBook Pros, Raspberry Pi's (new this upcoming year), and Parrot.AR 2.0 Quadcopters in some of the labs. The MacBooks are required as they house various pentesting tools (Kali Linux Virtual Machines, Cain & Abel, Metasploit, etc.) that are not allowed on their personally owned, government procured laptops. The drones are used as a physical target of cyber operations labs. They are designed to broadcast an 802.11 network, and

have inherently weak security. These labs are conducted in Leahy Hall, which has its own commercial internet access, unfiltered and unrestricted as the Mission Network (which will block search terms such as “hacking”).

APPENDIX D – INSTITUTIONAL SUMMARY

Programs are requested to provide the following information.

1. The Institution

a. Name and address of the institution

United States Naval Academy

b. Name and title of the chief executive officer of the institution

Vice Admiral Walter "Ted" Carter, Superintendent

c. Name and title of the person submitting the Self-Study Report.

Dr. Allen Parrish, Chair, Cyber Science Department

d. Name the organizations by which the institution is now accredited, and the dates of the initial and most recent accreditation evaluations.

Middle States Commission on Higher Education:

- initial accreditation 1947
- most recent accreditation 2011

2. Type of Control

Description of the type of managerial control of the institution, e.g., private-non-profit, private-other, denominational, state, federal, public-other, etc.

Federal

3. Educational Unit

Describe the educational unit in which the program is located including the administrative chain of responsibility from the individual responsible for the program to the chief executive officer of the institution. Include names and titles. An organization chart may be included.

The program is located within the Computer Science Department with the following administrative chain of responsibility:

VADM Walter Carter
Superintendent, United States Naval Academy

Dr. Andrew Phillips
Academic Dean and Provost

CAPT David Roberts, USN
Director, Division of Mathematics and Science

Dr. Allen Parrish, Professor
Chair, Cyber Science Department

4. Academic Support Units

List the names and titles of the individuals responsible for each of the units that teach courses required by the program being evaluated, e.g., mathematics, physics, etc.

Dr. Joseph Urban
Chemistry Department Chair

Dr. Michael Bilzor, CDR, USN
Computer Science Department Chair

Dr. Samara Firebaugh,
Electrical & Computer Engineering Department Chair

Dr. Mark McWilliams
English Department Chair

Dr. Rick Ruth
History Department Chair

Dr. Karen Flack
Mechanical Engineering Department Chair

Dr. Matt Testerman, CDR, USN
Political Science Department Chair

Dr. William Traves
Mathematics Department Chair

Dr. Charles Edmondson
Physics Department Chair

Dr. Bradley Bishop
Weapons and Systems Engineering Department Chair

5. Non-academic Support Units

List the names and titles of the individuals responsible for each of the units that provide non-academic support to the program being evaluated, e.g., library, computing facilities, placement, tutoring, etc.

Dr. Bruce Bukowski
Center for Academic Excellence, Director

Mr. Lou Gianotti
Information Technology Services Division, Director

Mr. Larry Clemens
Library, Director

6. Credit Unit

It is assumed that one semester or quarter credit normally represents one class hour or three laboratory hours per week. One academic year normally represents at least 28 weeks of classes, exclusive of final examinations. If other standards are used for this program, the differences should be indicated.

One semester credit-hour represents one class hour or two laboratory hours per week. One academic year represents 30 weeks of classes, exclusive of final examinations.

7. Tables

Complete the following tables for the program undergoing evaluation.

Table D-1. Program Enrollment and Degree Data

Cyber Operations

	Academic Year		Enrollment Year					Total Undergrad	Total Grad	Degrees Awarded			
			1st	2nd	3rd	4th	5th			Associates	Bachelors	Masters	Doctorates
Current Year	17	FT	-	54	31	45	-	130	-	-	45	-	-
		PT	-	-	-	-	-	-	-				
-1	16	FT	-	31	46	27	-	104	-	-	27	-	-
		PT	-	-	-	-	-	-	-				
-2	15	FT	-	57	28	-	-	85	-	-	-	-	-
		PT	-	-	-	-	-	-	-				
-3	14	FT	-	32	-	-	-	32	-	-	-	-	-
		PT	-	-	-	-	-	-	-				
-4	13	FT	-	-	-	-	-	-	-	-	-	-	-
		PT	-	-	-	-	-	-	-				

Give official fall term enrollment figures (head count) for the current and preceding four academic years and undergraduate and graduate degrees conferred during each of those years. The "current" year means the academic year preceding the on-site visit.

FT--full time
PT--part time

Table D-2. Personnel

Cyber Operations

Year[1]: 2017

	HEAD COUNT		FTE[2]
	FT	PT	
Administrative[2]	2	-	1
Faculty (tenure-track)[3]	5	3	5.9
Other Faculty (excluding student Assistants)	12	2	12.4
Student Teaching Assistants[4]	-	-	-
Technicians/Specialists	2	-	2
Office/Clerical Employees	1	-	1
Others[5]	-	-	-

Report data for the program being evaluated.

1. Data on this table should be for the fall term immediately preceding the visit. Updated tables for the fall term when the ABET team is visiting are to be prepared and presented to the team when they arrive.

2. Persons holding joint administrative/faculty positions or other combined assignments should be allocated to each category according to the fraction of the appointment assigned to that category.

3. For faculty members, 1 FTE equals what your institution defines as a full-time load

4. For student teaching assistants, 1 FTE equals 20 hours per week of work (or service). For undergraduate and graduate students, 1 FTE equals 15 semester credit-hours (or 24 quarter credit-hours) per term of institutional course work, meaning all courses — science, humanities and social sciences, etc.

5. Specify any other category considered appropriate, or leave blank.

APPENDIX E – COURSE NAMES IN THE CYBER OPERATIONS MATRIX

Fall Freshman Year

SC111-4 — Foundations of Chemistry I
SM121-4 — Calculus I
HE111-3 — Rhetoric and Introduction to Literature I
HH104-3 — American Naval History
SY110-3 — Fundamentals of Cyber Operations

Spring Freshman Year

NS101-2 — Fundamentals of Seamanship
SC112-4 — Foundations of Chemistry II
SM122-4 — Calculus II
HE112-3 — Rhetoric and Introduction to Literature II
FP130-3 — US Government and Constitutional Development
NL110-2 — Preparing to Lead

Fall Sophomore Year

NE203-3 — Ethics and Moral Reasoning for the Naval Leader
SP211-4 — Physics I
SM223-4 — Introduction to Applied Mathematics
HH215-3 — The West in the Premodern World
SY201-4 — Cyber Fundamentals I

Spring Sophomore Year

NN210-2 — Basic Navigation
SP212-4 — Physics II
HH216-3 — The West in the Modern World
SM242-4 — Discrete Mathematics for Cyber Operations
SY202-3 — Cyber Systems Engineering
SY204-4 — Systems Programming and OS Fundamentals

Fall Junior Year

NN310-3 — Advanced Navigation
EE301-4 — Electrical Fundamentals and Applications

HM/SS1-3 — Humanities/Social Science Elective
SY301-4 — Data Structures for Cyber Operations
SY303-4 — Applied Cyber Systems Architecture

Spring Junior Year

NL310-2 — Leadership Theory and Applications
HM/SS2-3 — Humanities/Social Science Elective
SY304-3 —Information Operations, Social Engineering, and Hacktivism
SY306-3 — Web and Database Cyber Operations
SY308-3 — Security: Fundamental Principles
SY310-4 — An Introduction to Networking and Wireless Communications

Fall Senior Year

NL400-2 — Law for the Junior Officer (Law of Armed Conflict)
ES300-3 — Naval Weapons Systems
EM300-4 — Principles of Propulsion
SY401-3 — Cyber Operations I
SY403-3 — Cyber Planning and Policy
SY4**-3 — Cyber Operations Elective

Spring Senior Year

NS43*-2 — Junior Officer Practicum
EA/N4**-4 — Aerospace Engineering or Naval Architecture and Ocean Engineering Elective
SY402-3 — Cyber Operations II
SY406-3 — Cyber Law and Ethics
SY4**-3 — Cyber Operations Elective

SIGNATURE ATTESTING TO COMPLIANCE

By signing below, I attest to the following:

That Cyber Operations (*Name of the program(s)*) has conducted an honest assessment of compliance and has provided a complete and accurate disclosure of timely information regarding compliance with ABET's *Criteria for Accrediting Computing Programs* to include the General Criteria and any applicable Program Criteria, and the ABET *Accreditation Policy and Procedure Manual.*

Andrew T. Phillips
Dean's Name (As indicated on the RFE)

26 June 2017

Signature **Date**