MEMORANDUM

TO: William Cohen
    Associate Provost and Dean for Undergraduate Studies

FROM: Elizabeth Beise
    Associate Provost for Academic Planning and Programs

SUBJECT: Proposal to Establish a Minor in Advanced Cybersecurity Experience for Students

At its meeting on September 4, 2015, the Senate Committee on Programs, Curricula and Courses approved the proposal to establish a minor in Advanced Cybersecurity Experience for Students. A copy of the proposal is attached.

The change is effective Spring 2016. Please ensure that the change is fully described in the Undergraduate Catalog and in all relevant descriptive materials.

MDC/
Enclosure

cc: Andrew Harris, Chair, Senate PCC Committee
    Barbara Gill, Office of Enrollment Management
    Reka Montfort, University Senate
    Erin Taylor, Division of Information Technology
    Pam Phillips, Institutional Research, Planning & Assessment
    Anne Turkos, University Archives
    Linda Yokoi, Office of the Registrar
    Cynthia Stevens, Office of Undergraduate Studies
    William Dorland, Honors College
Summary of Proposed Action:
This submission is a proposal for the creation of an ACES (Advanced Cybersecurity Experience for Students) minor. The ACES minor is a 16-credit program open to all upper-division UMD students, regardless of their majors. A complement to the highly successful ACES Honors College Citation program (which is open only to entering Honors College freshmen), the ACES minor offers technical grounding as well as interdisciplinary colloquia and seminars. A key requirement is experiential work on cybersecurity problems in the form of research, internships, or practical team projects supplied by business or governmental organizations.
Overview
Commerce, energy, banking, media, business operations, communications, and health care are all dependent on a secure, reliable digital information and communications infrastructure. Such systems are critical for effective functioning of society, thus information system threats—whether politically or criminally motivated—pose substantial and potentially catastrophic risks. To address this growing problem, many colleges and universities have increased the number of information security programs with a goal of graduating more cybersecurity specialists. Studies estimate that as many as 20,000 new cybersecurity professionals will be needed in the next 5-10 years in the Washington, DC metropolitan area alone (e.g., https://www.wantedanalytics.com/analysis/posts/how-will-6-000-cyber-security-jobs-affect-recruiting; http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf; http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf).

Yet, the multifaceted, complex nature of cybersecurity problems dictates that they cannot be resolved solely by increasing the number of technical specialists; technical solutions alone are insufficient to eliminate potential threats. Rather, there is pressing need for a variety of different professionals to understand and address cybersecurity problems from an interdisciplinary vantage point. Technical specialists need grounding in the criminological, financial, business, policy, defense, and legal aspects of threats in order to develop sound technical recommendations. Likewise, professionals in the areas of policy, law, media, business, and health care need sufficient understanding of technical issues to create multipronged policies and practices to protect vulnerable populations and systems.

The ACES (Advanced Cybersecurity Experience for Students) minor was developed specifically to address this critical interdisciplinary intersection. The ACES minor is a 16-credit program open to all upper-division UMD students, regardless of their majors. A complement to the highly successful ACES Honors College Citation program (which is open only to entering Honors College freshmen), the ACES minor offers technical grounding to non-engineering and non-computer science majors as well as interdisciplinary colloquia and seminars to all admitted students. A key requirement is experiential work on cybersecurity problems in the form of research, internships, or practical team projects supplied by business or governmental organizations. Entering cohorts of approximately 50 students would be admitted using Honors College admission criteria. Funding for the first three years of this program has been solicited from Northrop Grumman, which sponsored the ACES Honors College Citation program. Subsequent funding would be secured through student project proposals, continued support from Northrop Grumman, and at least 20 companies in the ACES Corporate Partner Program.

Mission and Purpose
- How does the program support the mission & strategic goals of UMD?
The most recent UMD strategic plan (Transforming Maryland – Higher Expectations) emphasizes the university’s commitment to attracting academically talented future leaders, improving graduation of students in STEM fields, and offering financial and community support for a diverse student body. The ACES minor offers potential to affect achievement of these goals in the following ways.

- The ACES minor offers an attractive degree option to our most academically talented students.
Experience with the ACES Honors Citation program has proven that significant interests exists among top entering freshmen: cohort size has nearly doubled over three years (from 57
students in 2013 to over 100 for the incoming class) with average GPAs of 4.5, average SAT scores over 1440, and more than 10% Banneker-Key scholarship recipients. Extrapolating this to the ACES minor program, we anticipate that a sizable percentage of these students will continue and be joined by transfer and other students eligible for Honors College admission.

- **STEM majors are typically less diverse than students from other parts of campus.** For example, IRPA data for 2013-2014 show that relative to campus as a whole (where women earned 48.9% of undergraduate degrees granted), graduates in Computer, Mathematical and Natural Science (42.7% female) and engineering (20.7% female) were overwhelmingly male. Relative to campus (where graduates were 10.3% African American and 7.5% Latino), undergraduates in CMNS (9.7% African American, 5.2% Latino) and engineering (5.5% African American, 4.9% Latino) also included fewer underrepresented minorities. Offering the ACES minor to students in all colleges opens possibilities for students in ARHU (60.7% women, 10.3% African American, 9.1% Latino), BSOS (50.1% women, 11.4% African American, 9.1% Latino), and Journalism (62.6% women, 9.7% African American) to gain grounding in the technical aspects of cybersecurity issues. This may improve their employability following graduation.

- **The ACES minor leverages UMD’s geographic location.** The College Park campus is uniquely situated within the cybersecurity community in its proximity to federal agencies such as NSA, the U.S. Cyber Command and NIST, major defense contractors such as Northrop Grumman and Lockheed Martin, and federal policy makers. The opportunities to cultivate internships, research projects, and organizational sponsorship of student team projects is much higher than that of other major research universities.

- **The ACES minor will offer a variety of global opportunities.** Currently a study abroad course in Australia (HACS408A: Global Perspectives on Cybersecurity—Australia) is planned and another in France (HACS208F: Global Perspectives on Cybersecurity—France) will launch shortly for ACES Honors Citation students. The latter can be easily expanded to include students in the ACES minor.

- **What related programs are currently offered in the state of Maryland? How does the proposed program differ in curriculum or addresses constituencies not served?**

As noted above, most current cybersecurity programs, including those in the state of Maryland, focus almost exclusively on the technical aspects associated with programming. (A complete list of such programs offered by other institutions in the state is show below.) For example, the **UMD computer science major-cybersecurity specialization** focuses exclusively on such courses; its requirements include the following:

- CMSC412: Operating Systems
- CMSC433: Programming Language Technologies and Paradigms
- CMSC414: Computer & Network Security
- CMSC456: Cryptology
- CMSC417: Computer Networks
- CMSC411 (Computer Systems Architecture) OR CMSC430 (Introduction to Compilers)
- CMSC420 (Data Structures) OR CMSC451 (Design & Analysis of Computer Algorithms)

In contrast to the UMD computer science specialization in cybersecurity and other in-state programs, **the ACES minor is unique** in that its focus is on interdisciplinary features of cybersecurity and it emphasizes experiential learning opportunities to ensure that students gain a broad systems perspective on cybersecurity problems. **No other such programs are currently offered in the state of Maryland.**
<table>
<thead>
<tr>
<th>Other State of Maryland Higher Education Institutions</th>
<th>Degree</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bowie State University</td>
<td>BS in Computer Technology with concentration in computer &amp; network security</td>
<td>127-130 credits</td>
</tr>
<tr>
<td>Capitol Technology University</td>
<td>BS in Cyber and Information Security</td>
<td>4 approved courses for minor</td>
</tr>
<tr>
<td>Towson University</td>
<td>BS in Computer Science, option of security track Combined major in Computer Science &amp; Math with security track Minor in Computer Science</td>
<td>5 courses from pre-approved list for minor</td>
</tr>
<tr>
<td>UMBC</td>
<td>Major and minor in Cybersecurity/ Information Assurance</td>
<td>25 credits focused on programming &amp; security</td>
</tr>
<tr>
<td>UMUC</td>
<td>Major and minor in Cybersecurity</td>
<td>36 credits focused on operating systems, networking, computer security &amp; cyber ethics</td>
</tr>
<tr>
<td>Anne Arundel Community College</td>
<td>Customized approach to building training programs in core &amp; specialized modules</td>
<td>18 core credits focused on computer systems + electives; 21 credits for certificate</td>
</tr>
<tr>
<td>Community College of Baltimore County</td>
<td>Information Systems Security degree &amp; certificate programs</td>
<td>18-21 credits pertaining to network security</td>
</tr>
<tr>
<td>Cecil College</td>
<td>Associate of Science, Cybersecurity option</td>
<td>36 credits focused on computers, networks &amp; defense</td>
</tr>
<tr>
<td>College of Southern Maryland</td>
<td>Associate of Applied Science, Information Systems Security</td>
<td>10 required courses</td>
</tr>
<tr>
<td>Frederick Community College</td>
<td>Associate of Applied Science, Information Technology; Certificate in Information Security &amp; Assurance</td>
<td>part-time, 1 year graduate credit program</td>
</tr>
<tr>
<td>Howard Community College</td>
<td>Associate of Science in Network Security or Associate of Applied Science, Network Administration</td>
<td></td>
</tr>
<tr>
<td>Montgomery College</td>
<td>Cybersecurity Associate of Applied Science</td>
<td></td>
</tr>
<tr>
<td>Prince Georges Community College</td>
<td>Cybersecurity Associate of Applied Science</td>
<td></td>
</tr>
<tr>
<td>Loyola University of Maryland</td>
<td>Cybersecurity certificate</td>
<td></td>
</tr>
</tbody>
</table>

- What evidence is there that the state needs or market demands graduates?

According to the U.S. Department of Labor (http://www.onetonline.org/link/summary/15-1122.00), 2012-2022 projected growth in the job classification of information security analysts will be much faster than average, with projected openings estimated to increase by 37% nationwide and 14% in the state of Maryland. Median wages in the state of Maryland are estimated to be $95,500 with a low end of $55,400 and a high end of $148,700. Recall that some portion of ACES minor students will specialize in technical areas beyond their interdisciplinary breadth and thus benefit from the projected demand for these graduates.
Labor Department projections are not sufficiently fine-grained to estimate demand for professionals in disciplines such as government and politics, law, criminology, public policy, business, journalism, or linguistics who possess a solid grasp of cybersecurity implications and have practical experience working on such problems. If we extrapolate from the high demand for cybersecurity professionals generally, it appears that an interdisciplinary minor degree may make such graduates more attractive within these impacted disciplines.

- **What data shows student interest in the program?**
42 students have applied for admission to the ACES minor in Fall 2015; of these, 31 are ACES Honors Citation students, showing that 69% of students wish to continue. Using this base rate with the current freshmen cohort of 66 students, we could expect that at least 45 are likely to apply for Fall 2016. Projecting further from the incoming ACES Honors Citation cohort (currently at 106 students), we anticipate 73 ACES minor students for Fall 2017. It is highly likely that a larger number of non-ACES Honors Citation students may apply in Fall 2016 once the ACES minor has been established and advertised more broadly on campus.

We anticipate about 50 students in the ACES minor for the first two years. In parallel we will develop sources of external support so that we can accommodate a larger student population (75-100) over the coming years.

**Characteristics of Proposed Program**

- **Educational objectives of program**
The ACES minor curriculum consists of advanced coursework in cybersecurity and provides students with an opportunity to get a deeper exposure to specific aspects of cybersecurity. The mission of the ACES Honors College Citation program is to provide students with a foundation in cybersecurity (HACS 100 and 102), two seminars on broad topics in cybersecurity (HACS 208), and three credits of experiential learning. In the ACES minor, non-ACES Honors College Citation students would first need to take (depending on their background) one or two prerequisite courses in cybersecurity (HACS 201 and 202) to ensure sufficient technical understanding. The ACES minor consists of at least nine credits of advanced coursework in cybersecurity (HACS 402, 404, 408 or authorized substitutes), three to six credits of experiential learning, and a one-credit cybersecurity experts colloquium course. Students may choose to complete the minimum required 16 credits with courses, an internship, research experience, or a company-sponsored cybersecurity project.

The academic curriculum for the ACES minor is designed to meet the following learning outcomes:

1) Students will demonstrate the ability to apply advanced technical skills required to approach and resolve problems in cybersecurity through upper-level cybersecurity-related coursework in computer science, engineering, and related disciplines.

2) Students will be able to apply the broad interdisciplinary aspects of cybersecurity, such as the criminological, political, legal, and economic ramifications of local and global cybersecurity advances and decisions.

3) Students will obtain hands-on experience and demonstrate problem-solving skills in cybersecurity through advanced coursework, experiential learning, and research.

4) Students will gain sophisticated understanding of the range of professional opportunities available in cybersecurity as a result of first-hand interactions with cybersecurity professionals in the private and public sectors through formal presentations, site visits, informal meals, and topical and professional workshops.
• **Title for Transcript**

ACES (Advanced Cybersecurity Experience for Students) Minor

• **Primary Sponsoring Unit**

Honors College (HC), Office of Undergraduate Studies (UGST)

• **Brief catalog description**

The Undergraduate Minor in Advanced Cybersecurity Experience for Students is a cross-disciplinary program open to students in all majors and housed in the Honors College within the Office of Undergraduate Studies (UGST). The minor takes a multidisciplinary approach to cybersecurity in which students gain knowledge about many of the fields (criminal justice, business, public policy) that intersect in cybersecurity. With an emphasis on hands-on experiences, students will gain practical skills through coursework, seminars, group projects, internships, and research, both on and off campus. Students will also have the opportunity to participate as peer mentors, tutors, and advisors. The minor program will also include regular interactions with corporate and governmental leaders in cybersecurity, who will serve as both mentors and professional contacts. Following admission to the program and completion of prerequisites for non-ACES I students, **minimum of 16 credit hours is required**. Of these, at least 9 credits must be in junior- or senior-level seminars, a semester-long 1-credit colloquium is required, and students must complete at least 3 credits of experiential learning.

• **Program Oversight**

The current ACES program is housed in the Honors College (HC) in the Office of Undergraduate Studies (UGST). As such, the ACES minor will be overseen by the HC Executive Director and the UGST Dean.

The ACES minor will be led by the current ACES Honors Citation team:

- Michel Cukier, Director
- Jandelyn Plane, Associate Director
- William Nolte, Director of Outreach
- Elizabeth Galvin, Coordinator

An Interdisciplinary Leadership Council, composed of faculty members of the colleges involved in ACES, will advise on curriculum development, potential instructors for the program, admissions criteria, and student plans for completion of the program.

• **General requirement for degree including total number of credits & their distribution**

The ACES minor curriculum consists of advanced coursework in cybersecurity and is designed to build on the ACES Honors Citation program, which was launched in 2012. The ACES minor offers students across campus an opportunity to gain a deeper exposure to specific aspects of cybersecurity. The following table shows the Honors College ACES Citation and ACES minor curricula.

<table>
<thead>
<tr>
<th></th>
<th>Honors College ACES Citation (freshmen/sophomores)</th>
<th>ACES Minor (juniors/seniors)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Hours</td>
<td>14 credits, Honors College Citation</td>
<td>Minimum of 16 credits after completing either ACES I or after completing HACS 201 and 202</td>
</tr>
<tr>
<td><strong>Honors College ACES Citation (freshmen/sophomores)</strong></td>
<td><strong>ACES Minor (juniors/seniors)</strong></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Prerequisites</strong>&lt;sup&gt;1&lt;/sup&gt;</td>
<td>HACS201 Introduction to Unix (1 credit; for non-ACES I students who have not taken CMSC216)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HACS202 Group project in Cybersecurity (3 credits; for non-ACES I students)</td>
<td></td>
</tr>
<tr>
<td><strong>Required Courses</strong></td>
<td>HACS318 Cybersecurity Professionals Colloquium Series (1 credit; all students take at least one semester)</td>
<td></td>
</tr>
<tr>
<td>HACS100 Foundations of Cybersecurity (2 credits)</td>
<td>HACS208 ACES I seminar courses will be available to ACES II students on a seat-available basis.</td>
<td></td>
</tr>
<tr>
<td>HACS102 Foundations of Cybersecurity (3 credits, prerequisite HACS100)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Optional Enrichment Courses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Course Options</strong></td>
<td>Take at least THREE of the following 400-level courses:</td>
<td></td>
</tr>
<tr>
<td>Choose two seminars for total of 6 credits</td>
<td>HACS402 Applied Security Analysis &amp; Visualization (3 credits)</td>
<td></td>
</tr>
<tr>
<td>HACS208 Seminar in Cybersecurity (3 credits each)</td>
<td>HACS404 Security through Cyber Forensics (3 credits)</td>
<td></td>
</tr>
<tr>
<td>• A. Accounting &amp; Economic Aspects</td>
<td>HACS408 Advanced Seminar in Cybersecurity (3 credits) these will include special topics seminars comparable to those offered at the 200-level&lt;sup&gt;2&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td>• C. Human Actors &amp; Cyber Attacks</td>
<td>• A: A Global Perspective on Cybersecurity – Australia</td>
<td></td>
</tr>
<tr>
<td>• E. Introduction to Reverse Engineering</td>
<td>• B*: Security Incident Handling and Response</td>
<td></td>
</tr>
<tr>
<td>• F: A Global Perspective on Cybersecurity – France</td>
<td>• C*: Cloud and Data Center Security</td>
<td></td>
</tr>
<tr>
<td>• C. Human Actors &amp; Cyber Attacks</td>
<td>• D*: Mobile &amp; Consumer Device Security</td>
<td></td>
</tr>
<tr>
<td>• G. Privacy versus In-Your-Face Big Government</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• N. National Security Dilemmas</td>
<td>Students may also substitute 1 or 2 of the following 400-level courses&lt;sup&gt;3&lt;/sup&gt;: CCJS418B, CMSC414,</td>
<td></td>
</tr>
<tr>
<td>• P. Beyond Technology, Policy Implications of Cyberspace</td>
<td>CMSC456, CMSC498B, CMSC498R, ENEE459C,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ENEE459D, ENEE459E, ENME442</td>
<td></td>
</tr>
<tr>
<td><strong>Experiential Learning</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Take 3 credits from the following options</td>
<td>Take at least THREE but not more than SIX credits from the following options:</td>
<td></td>
</tr>
<tr>
<td>HACS279 Undergraduate Research in Cybersecurity (1-3 credits) or HACS287</td>
<td>HACS479 Undergraduate Research in Cybersecurity (1-3 credits, repeatable up to a maximum of 6 credits)</td>
<td></td>
</tr>
<tr>
<td>Undergraduate Research in Cybersecurity (3 credits)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HACS297 Cybersecurity Experience Reflection on Internship Learning (3 credits)</td>
<td>HACS498 Cybersecurity Team Problem Solving Experience (3 credits, repeatable up to a maximum of 6 credits)</td>
<td></td>
</tr>
</tbody>
</table>

- **List of courses by title and number, including prerequisites**

Other than some potential technical HACS408 topics, ACES minor classes will not have a prerequisite. Note that students who were not in the Honors College ACES Citation program and who have not taken CMSC216 must take HACS201 to ensure that they have sufficient understanding of technical issues. All

---

<sup>1</sup> Students who were not in the Honors College ACES Citation program and are in a non-technical major will need basic computing skills in order to work on projects with technically oriented students. Two “bridge” courses will be prerequisites for such students and do not count toward either the notation or the minor. Non-Honors College ACES Citation program students would be conditionally admitted in fall semester and take these prerequisites in the spring each year.

---

<sup>2</sup> Courses shown with an asterisk have not yet been developed but are slated pending program approval.

---

<sup>3</sup> Only students with the right prerequisites could take these courses. If some of these courses are restricted to students from specific departments/colleges, then only these students in the ACES minor would be allowed to take these courses as substitutes.
students who were not in the Honors College ACES Citation program must take HACS202 so that they gain experience working in interdisciplinary teams on cybersecurity problems.

**HACS201: Introduction to UNIX**
Course Description: Introduction to the operating system UNIX through lectures and hands-on assignments.

**HACS202: Group Project in Cybersecurity**
Course Description: The group project in this course will combine technical, analytical, and communication skills, further engaging students in the practice of cybersecurity. Students will learn about design concepts and data analysis as they engage in a team project designing, deploying, and collecting and analyzing data from a honeypot. The hands-on nature of the course will give students experiential insight about how and why attackers attack and how to engage in protective measures to prevent attacks.

**HACS402: Applied Security Analysis and Visualization**
Course Description: This class discusses various security datasets including network traffic, firewall logs, intrusion detection system events, vulnerability data, security incidents, and email data.

**HACS404: Security through Cyber Forensics**
Course Description: This course introduces digital investigations and discusses the systematic approach of investigating a crime. Computer and network forensics are discussed. Basic forensic scientific concepts are presented at the computer level and applied for Windows, Unix, Macintosh and mobile systems.

**HACS408: Advanced Seminar in Cybersecurity**
Course Description: The Advanced Seminar in Cybersecurity explores various lenses of cybersecurity in order to promote an interdisciplinary understanding of the field. Although each section may focus on a different topic, each integrates active student engagement, communication, critical thinking, and teamwork.

- **A: A Global Perspective on Cybersecurity – Australia**
  Course Description: This 3 week study abroad course explores cybersecurity in Australia from the technical, cultural, political, and economic perspectives, as well as solutions developed through innovation and technology. While in Australia, students will participate in lectures, field trips, journaling assignments, student presentations, an oral and written exam, and engage in discussions among students, faculty, site visit hosts, and people we meet.

- **B: Security Incident Handling and Response**
  Course Description: This course develops core skills required for security professionals to handle security incidents from both a technical and legal capacity. Core content areas include identifying affected assets and users involved in an incident, attributing attackers involved with the compromise, mitigating the current attack, and developing an action plan to prevent such future attacks.

- **C: Cloud and Data Center Security**
  Course Description: This course is a team based learning experience where students work with faculty and industry partners to design prototypes in security improvements to cloud and large-scale computing environments. Core course content includes drafting and prototyping unique solutions to challenges currently being faced by the computer industry.

- **D: Mobile & Consumer Device Security**
Course Description: This course delves into the complex threats that impact millions of mobile devices around the world, including common platforms such as Android and iOS, as well as wearable devices and Internet of Things (IoT) devices. Students will gain hands on experience in exploitation techniques to common consumer devices in the market, and will learn data forensics techniques as it applies to mobile devices.

**HACS479: Undergraduate Research in Cybersecurity**
Course Description: The Advanced Cybersecurity Experience for Students (ACES) program encourages its students to engage in research in order to gain greater insight into a specific area within cybersecurity, obtain an appreciation for the subtleties and difficulties associated with the production of knowledge and fundamental new applications, and prepare for graduate school and the workforce.

**HACS498: Cybersecurity Team Problem Solving Experience**
Course Description: This course provides ACES II students with an opportunity to learn in multidisciplinary teams in a real-world setting. Companies engage teams of ACES students with real organizational challenges in cybersecurity. These companies dedicate resources to help students address these difficult problems. Student teams must design, implement and evaluate a security solution.

- **Expected learning outcomes**
  1) Students will demonstrate the ability to apply advanced technical skills required to approach and resolve problems in cybersecurity through upper-level cybersecurity-related coursework in computer science, engineering, and related disciplines.
  2) Students will be able to apply the broad interdisciplinary aspects of cybersecurity, such as the criminological, political, legal, and economic ramifications of local and global cybersecurity advances and decisions.
  3) Students will obtain hands-on experience and demonstrate problem-solving skills in cybersecurity through advanced coursework, experiential learning, and research.
  4) Students will gain sophisticated understanding of the range of professional opportunities available in cybersecurity as a result of first-hand interactions with cybersecurity professionals in the private and public sectors through formal presentations, site visits, informal meals, and topical and professional workshops.

- **Program faculty and their credentials, explain advising structure for the program**
The ACES minor will be led by the ACES team, their credentials are described in more detail below:

**Michel Cukier:**
Dr. Cukier is the Director for Advanced Cybersecurity Experience for Students (ACES) and the Associate Director for Education for the Maryland Cybersecurity Center (MC2). Michel is an Associate Professor of Reliability Engineering with a joint appointment in the Department of Mechanical Engineering at the University of Maryland, College Park. Michel received a degree in physics engineering from the Free University of Brussels, Belgium, in 1991, and a doctorate in computer science from the National Polytechnic Institute of Toulouse, France, in 1996. From 1996 to 2001, he was a researcher in the Perform research group in the Coordinated Science Laboratory at the University of Illinois, Urbana-Champaign. He joined the University of Maryland in 2001 as Assistant Professor. His research covers dependability and security issues. His latest research focuses on the empirical quantification of cybersecurity. He has published over 70 papers in journals and refereed conference proceedings in those areas.
Jandelyn Plane:
Dr. Plane is Director of the new Maryland Center for Women in Computing at UMCP, Associate-Director of ACES (the first undergraduate cybersecurity honors program), and Advisor to the Association for Women in Computing (grad/undergrad student group). For 15 years, she worked on university computer science capacity building projects in sub-Saharan Africa and Afghanistan. Jan holds graduate degrees in both computer science and education; her work focuses on computer science curriculum, pedagogical methods and underrepresented populations in computing. She encourages both quality of content and access to computing for students (middle-school to graduate-school) through teaching, outreach programs and teacher professional development.

William Nolte:
Dr. Nolte is the former director of education and training in the office of the Director of National Intelligence and chancellor of the National Intelligence University. He is a former Deputy Assistant Director of Central Intelligence, Central Intelligence Agency. He was Director of Training, Chief of Legislative Affairs and Senior Intelligence Advisor at the National Security Agency. He also served as Deputy National Intelligence Officer for the Near East and South Asia during the Gulf War. He has taught at several Washington area universities, is on the board of CIA's Studies in Intelligence, and directed the Intelligence Fellows Program.

Elizabeth Galvin:
Elizabeth Galvin serves as the Coordinator for the ACES Honors Program in the Honors College at the University of Maryland. In her current role, Elizabeth coordinates experiential and extracurricular programming, recruitment and orientation of new students, and advises the ACES Student Board leadership group. Elizabeth received her B.A. in French Language & Literature at the University of Maryland, spending her junior year abroad on the Maryland-in-Nice program. She is also an Honors College alumna, having completed the University Honors Program. She then went on to receive her M.A. in Higher Education Administration from Columbia University. Prior to joining ACES, Elizabeth worked in several areas of higher education, including Undergraduate Admissions and Education Abroad.

The students in the ACES minor will be advised by the ACES Director, Associate Director and Assistant Director. An Interdisciplinary Leadership Council, composed of faculty members of the colleges involved in ACES, will advise on curriculum development, potential instructors for the program, admissions criteria, and student plans for completion of the program.

The ACES minor consists of HACS201, 202, 402, 404, 408, 318, 479 and 498. HACS318 is the Cybersecurity Professionals Colloquium Series course that will be administered directly by the ACES team.

HACS201, 202, 402 and 404 are expected to be taught by ACES instructors who have not yet been hired.

HACS408 courses are expected to mostly be taught by governmental or corporate security experts. The ACES Honors College Citation program has instructors from UMD and from external institutions. HACS208A, HACS 208C, and HACS208P are respectively being taught by UMD Prof. Lawrence Gordon (BMGT), UMD Dr. Katherine Izsak (BSOS/START), and UMD Dr. William Nolte (PUAF). HACS208E - Reverse Engineering, is being taught by Daniel Buettner, a researcher at the Laboratory for Telecommunication Sciences (LTS, an NSA lab). HACS208Z - Methods for Solving (and Not Solving)
Puzzles is being taught by Dimitrije Kostic (researcher at LTS) and Greg Clark (NSA employee). The ACES program is currently reaching out to additional instructors at UMD and from governmental and corporate institutions to develop and teach relevant courses.

For HACS479, the advisors will be faculty from the Maryland Cybersecurity Center (MC2). The following website lists these faculty and their credentials: http://www.cyber.umd.edu/faculty.

For HACS498, student teams will be advised jointly by a governmental or corporate security expert and either an ACES staff member or an MC2 faculty member.

- **Student audience to be served by program with enrollment estimates**
The ACES minor will be open to all upper division students on campus who meet Honors College admission criteria. The program as currently designed and staffed is equipped to handle 50 students each during the first two years. As external sources of support are cultivated, the yearly number of admitted students can increase to 75-100.

The number of students admitted to the ACES Honors Citation program has increased by more than 80% over the past three years, from 57 to 106 for Fall 2015. Given the interest in that program, we anticipate similar strong interest in the ACES minor. Preliminary numbers support this idea. As of March 2015, 42 students applied for admission to the ACES minor in Fall 2015; of these, 31 students are ACES Honors Citation students, indicating a 69% continuation rate. This yields estimates of 45 ACES Honors Citation students in 2016 and 73 Honors Citation students for Fall 2017. Given that the program has not yet been approved or advertised broadly, it seems likely that a larger number of non-ACES Honors Citation students may apply once the ACES minor has been established.

- **Procedures for admitting students into the minor**
The ACES minor will be a two year program of advanced study in cybersecurity for juniors and seniors. Students will apply during their sophomore year to enter the program in the fall of their junior year and must meet all of the following requirements at the time of application to be eligible for consideration:
  
  - Minimum of 30 university credits completed (sophomore standing; not including AP/IB credits);
  - Strong academic record (minimum GPA of 3.0); and
  - At least four semesters remaining at the University of Maryland prior to graduation.

Students of all majors will be eligible to apply and prior admission to the Honors College will not be required. Although there are no pre-requisite courses for participation, ACES staff will recommend that students have completed at least one or more of the following:
  
  - Completion of the Honors College Citation in Cybersecurity;
  - Completion of relevant introductory coursework, including one or more of the following, with a grade of B or better:
    - Calculus I (MATH130, MATH140, MATH220)
    - Introductory Statistics (including STAT100, BMGT230, CCJS200, PSYC200, SOCY201, AP Statistics, etc.)
    - CMSC131 Object-Oriented Programming I
    - ENES100 Introduction to Engineering Design; and
  - Previous practical experience (such as internships and/or research) related to cybersecurity.

- **Impact on students technology fluency**
Students in the ACES minor will become more fluent in technologies involved in cybersecurity through: 1) the advanced technical courses (HACS402, HACS404 and the technical topics of HACS408), and 2) the 3-6 credits of experiential learning in cybersecurity.

- Facilities requirements & equipment
  Facilities and equipment required for launching the ACES Honors Citation program were funded by Northrop Grumman. Currently, the provost is developing a plan to cover lab facilities for ACES minor students.

- Description of proposed means of offering the program (any components offered off-campus, online, in cooperation with another institution or through non-traditional schedule?)
  Besides HACS201 that will be offered over a 5 week period, all other courses are expected to be offered using a traditional schedule.

- Reliance on courses provided through other academic units—list the required courses & prerequisites along with letters from chairs or deans committing necessary seats
  There is no required course from other academic units. Two relevant courses from other units (as determined by program staff) may count as electives towards the minor.

- Library resources required—need letter from librarian staff describing collection needs
  Many resources regarding cybersecurity are now directly available on-line. The UMD library has purchased the access rights to all IEEE and ACM journals and conferences. Most articles in cybersecurity are published by IEEE or ACM. In addition the UMD library provides access to the Compendex and INSPEC databases where additional articles on cybersecurity can be searched.
Fwd: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Michel Cukier <mcukier@umd.edu>  Fri, May 22, 2015 at 7:38 AM
To: stevensc-contact <cstevens@rhsmith.umd.edu>

FYI.

Sent from my iPad

Begin forwarded message:

From: "B Balachandran" <balab@umd.edu>
To: "Michel Cukier" <mcukier@umd.edu>
Cc: "Kenneth T. Kiger" <kkiger@umd.edu>, "Terry L. Island" <tisland@umd.edu>, "Hugh Alan Bruck" <bruck@umd.edu>
Subject: Fwd: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Dear Michel:

In response to your e-mail, based on the feedback received from the Undergraduate Office of the Department, we provide our approval for this substitution. As we proceed further, please keep our Undergraduate Office and the unit informed.

With best wishes,

Bala.

____________________________
B. Balachandran
Chair and Minta Martin Professor
Department of Mechanical Engineering
Faculty Member, Applied Mathematics and Scientific Computation
University of Maryland
College Park, MD 20742-3035
PH: (301)405-5309; (301)405-4747 (Chair's Office)
FAX: (301)314-9477
E-mail: balab@umd.edu<mailto:balab@umd.edu>

-------- Forwarded Message --------
Dear Bala:

The purpose of this email is to obtain the approval to list the following class, ENME442, as a substitute for one course of the ACES minor.
Please find attached the proposal of the ACES minor. Pages 6-7 list the courses included in the proposed minor. We would like to list ENME442 as a substitute for one course of the ACES minor. We do not anticipate more students taking this class due to the listing as a substitute in the ACES minor. Could you please confirm that you allow us to list ENME442 as a substitute for one course of the ACES minor.

Thank you in advance.

Regards,

Michel

---

Michel Cukier
Director, Advanced Cybersecurity Experience for Students (ACES)
Associate Director for Education, Maryland Cybersecurity Center (MC2)
Associate Professor, Reliability Engineering
Department of Mechanical Engineering
University of Maryland
3419 A.V. Williams Building
College Park, MD 20742
Phone: 301-314-2804
Email: mcukier@umd.edu
URL: http://terpconnect.umd.edu/~mcukier/

2 attachments

- DRAFT proposal for ACES minor-simplified 0511.pdf
  710K
- ATT00001.htm
  1K
FW: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Michel Cukier <mcukier@umd.edu>
To: stevensc-contact <cstevens@rhsmith.umd.edu>

FYI.

From: Alan Sussman [als@cs.umd.edu]
Sent: Wednesday, May 20, 2015 3:20 PM
To: Michel Cukier
Cc: samirk-contact
Subject: Re: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

We're OK with the courses, Michel.

As I said previously, the only concern from our side is that it looks very easy for a CS ACES I student to do this minor. But I think that is the intent, right?

Alan

On 05/20/2015 09:03 AM, Michel Cukier wrote:
> Dear Samir and Alan,
> 
> Do you have any questions? Do you want to meet so that I give you details? I am leaving on Saturday for a Study Abroad course and was asked to get the proposal package done in the next days. Thank you.
> 
> Regards,
> 
> Michel
> 
> > From: Michel Cukier
> > Sent: Monday, May 18, 2015 9:19 AM
> > To: Alan Sussman
> > Cc: samirk-contact; Michel Cukier
> > Subject: RE: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal
> > 
> > Dear Samir and Alan,
> > 
> > I just need your approval that the CS courses I listed in the proposal can be double counted. Up to 6 credits in a minor can be double counted. We have identified cybersecurity related classes in CCJS, ME, ECE and CS. Thus, we have reached out to each of these departments to get their approval of having the classes we listed as double counted. Does it answer your question?
> > 
> > For non-ACES I students, they need to take HACS 202. HACS 201 needs to be taken by any student who has no background in Unix (i.e., students who have not taken CMSC 216). Does it answer your question?
> > 
> > Please let me know if you have any additional question/comment. Just a reply via email that you approve the list of courses is enough. Thank you.
> > 
> > Regards,
From: Alan Sussman [als@cs.umd.edu]
Sent: Friday, May 15, 2015 5:54 PM
To: Michel Cukier
Cc: samir-k-contact
Subject: Re: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Michel,

Samir and I talked for a little bit this afternoon, and we have one big question. That follows, but we also want to know what you really want from us? Is it to support the proposal as it goes through the PCC process?

The question relates to how the minor will work for CS students, especially ones who go through the ACES I living/learning honors program. If we're reading your proposal correctly, if those students take CMSC414 and CMSC456, then to do the minor they'd need to take one of the HACS 40X classes, and one experiential learning class (a total of 6 credits). For a CS non-ACES I student, they'd also need to take HACS201 and HACS202, right?

I'll be in the office most of next week to talk more about this. I think Samir will be around most of the week too.

Alan

On 05/13/2015 01:16 PM, Samir Khuller wrote:

> Dear Michel,
> I immediately sent the email to Alan as I am on travel and with a pretty packed schedule. Can you talk to him today? I get back on Thu morning and can discuss with him tomorrow.
> Sorry for the delay.
> samir
>
> On Wed, 13 May 2015, Michel Cukier wrote:
> >>> Dear Samir:
> >>> Please let me know if you wanted to meet so that I can answer any question you have about the proposal. Thank you.
> >>> Regards,
> >>> Michel
> >>>
From: Michel Cukier
Sent: Monday, May 11, 2015 11:30 AM
To: Samir Khuller
Cc: Michel Cukier
Subject: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Dear Dr. Khuller:

The purpose of this email is to obtain the approval to list the following classes, CMSC414, CMSC456, CMSC498B, CMSC498R, as substitutes for one or two courses of the ACES minor.

Please find attached the proposal of the ACES minor. Pages 6-7 list the courses included in the proposed minor. We would like to list CMSC414, CMSC456, CMSC498B, CMSC498R as substitutes for one or two courses of the ACES minor. We do not anticipate more students taking these classes due to the listing as substitutes in the ACES minor. Could you please confirm that you allow us to list CMSC414, CMSC456, CMSC498B, CMSC498R as substitutes for one or two courses of the ACES minor.

Thank you in advance.

Regards,

Michel

Director, Advanced Cybersecurity Experience for Students (ACES)
Associate Director for Education, Maryland Cybersecurity Center (MC2)
Associate Professor, Reliability Engineering
Department of Mechanical Engineering
University of Maryland
3419 A. V. Williams Building
College Park, MD 20742
Phone: 301-314-2804
Email: mckier@umd.edu
URL: http://terpconnect.umd.edu/~mckier/
FYI.

From: James Lynch
Sent: Monday, May 11, 2015 5:30 PM
To: Michel Cukier
Subject: RE: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Yes.

From: Michel Cukier
Sent: Monday, May 11, 2015 11:19 AM
To: James Lynch
Cc: Michel Cukier
Subject: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Dear Dr. Lynch:

The purpose of this email is to obtain the approval to list the following class, CCJS418B, as a substitute for one course of the ACES minor.

Please find attached the proposal of the ACES minor. Pages 6-7 list the courses included in the proposed minor. We would like to list CCJS418B as a substitute for one course of the ACES minor. We do not anticipate more students taking this class due to the listing as a substitute in the ACES minor. Could you please confirm that you allow us to list CCJS418B as a substitute for one course of the ACES minor.

Thank you in advance.

Regards,

Michel
Michel Cukier
Director, Advanced Cybersecurity Experience for Students (ACES)
Associate Director for Education, Maryland Cybersecurity Center (MC2)
Associate Professor, Reliability Engineering
Department of Mechanical Engineering
University of Maryland
3419 A.V. Williams Building
College Park, MD 20742
Phone: 301-314-2804
Email: mcukier@umd.edu
URL: http://terpconnect.umd.edu/~mcukier/
FYI.

From: Ramirez, Neruh [nram@ece.umd.edu]
Sent: Tuesday, June 09, 2015 4:58 PM
To: Michel Cukier
Cc: Rama Chellappa; Donald Yeung
Subject: Re: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Hello Michel,

This looks great and yes, it does address our concern. Thanks for adding that information.

- Neruh

Mr. Neruh Ramirez
Director of Undergraduate Studies
Department of Electrical & Computer Engineering
A. James Clark School of Engineering
University of Maryland

PH: (301) 405-3685 | FAX: (301) 314-6082
E-mail: nram@umd.edu

Visit us online at: www.ece.umd.edu

On Tue, Jun 9, 2015 at 5:34 AM, Michel Cukier <mcukier@umd.edu> wrote:

Hi Neruh,

Please find attached the revised version with a footnote on page 6 (in yellow). Does it address your concern? Feel free to make any edit. Thank you.

Regards,
Michel

From: Ramirez, Neruh [nram@ece.umd.edu]  
Sent: Thursday, June 04, 2015 9:54 AM

To: Michel Cukier  
Cc: Rama Chellappa; Donald Yeung  
Subject: Re: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Michel,

Yes. I think it is a good idea to put this in the approval. I will be on the lookout for your e-mail. Thanks.

- Neruh

Mr. Neruh Ramirez  
Director of Undergraduate Studies  
Department of Electrical & Computer Engineering  
A. James Clark School of Engineering  
University of Maryland

PH: (301) 405-3685 | FAX: (301) 314-6082  
E-mail: nram@umd.edu

Visit us online at: www.ece.umd.edu

On Thu, Jun 4, 2015 at 9:16 AM, Michel Cukier <mcukier@umd.edu> wrote:

Hi Neruh,

So your recommendation is that I add such statement in the proposal and then send it back to you for approval, right? Thank you.

Regards,

Michel

From: Ramirez, Neruh [nram@ece.umd.edu]  
Sent: Thursday, June 04, 2015 9:09 AM
To: Michel Cukier  
Cc: Rama Chellappa; Donald Yeung  
Subject: Re: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Hello Michel,

Thanks for the explanation. I thought this was the case, but just wanted to make sure. If I may, I would recommend that you add something in the wording about course substitution that students will need to be eligible to take the substitute courses. Thanks.

- Neruh

Mr. Neruh Ramirez  
Director of Undergraduate Studies  
Department of Electrical & Computer Engineering  
A. James Clark School of Engineering  
University of Maryland  

PH: (301) 405-3685 | FAX: (301) 314-6082  
E-mail: nram@umd.edu  

Visit us online at: www.ece.umd.edu

On Thu, Jun 4, 2015 at 1:02 AM, Michel Cukier <mcukier@umd.edu> wrote:

Hi Neruh,

The request is only to have students who are allowed to take these ECE courses to have them counted towards the ACES minor. So only students with the right prereqs could take these courses. And if you have restricted these courses to only ECE students, then only ECE students in the ACES minor would be allowed to take these courses as substitutes. Does it answer your question? Thank you.

Regards,

Michel

From: Ramirez, Neruh [nram@ece.umd.edu]  
Sent: Wednesday, June 03, 2015 1:12 PM  
To: Michel Cukier  
Cc: Rama Chellappa; Donald Yeung  
Subject: Re: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal
Hello Michel,

Sorry for my delayed response, I hope all is going well with your program in France. In discussing your e-mail, we wanted to know if the course replacements (ENEE459C, ENEE459D, and ENEE459E) would only apply to ECE students in the ACES minor or if this is something that would be open to all ACES minor students. If the replacement is an option only for ECE students, then there is no issue. If the course replacement is an option for all ACES students, then we would need to have further discussion on how to handle the enrollment of non-ECE ACES students. Those are basically our concerns, let me know if you have additional questions about them. Thanks.

- Neruh

Mr. Neruh Ramirez
Director of Undergraduate Studies
Department of Electrical & Computer Engineering
A. James Clark School of Engineering
University of Maryland

PH: (301) 405-3685 | FAX: (301) 314-6082
E-mail: nram@umd.edu

Visit us online at: www.ece.umd.edu

On Wed, Jun 3, 2015 at 4:14 AM, Michel Cukier <mcukier@umd.edu> wrote:

Hi Neruh,

Can you please share your suggestions. Thank you.

Regards,

Michel

---

From: Michel Cukier
Sent: Sunday, May 31, 2015 9:46 AM
To: Rama Chellappa
Cc: Neruh Ramirez; Michel Cukier
Subject: RE: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal
Dear Rama,

Thank you!

Regards,

Michel

Dear Neruh,

Please let me know your concerns. Note that I am currently running HACS 208F in France. Thank you.

Regards,

Michel

---

From: Rama Chellappa [Rama@umiacs.umd.edu]
Sent: Wednesday, May 20, 2015 3:39 PM
To: Michel Cukier
Cc: Neruh Ramirez
Subject: RE: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Hi Michel;

Neruh Ramirez, Director of UG Studies has some suggestions.

Neruh:

please contact Michel.

Rama

---

From: Michel Cukier <mcukier@umd.edu>
Sent: Wednesday, May 20, 2015 3:17 PM
To: Ramalingam Chellappa
Cc: Michel Cukier
Subject: RE: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Dear Rama:

Please let me know if you have any question regarding the request and/or the proposal. Thank you.

Regards,

Michel

From: Michel Cukier
Sent: Wednesday, May 13, 2015 10:06 AM
To: Rama Chellappa
Cc: Michel Cukier
Subject: RE: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Dear Rama:

Please let me know if you wanted to meet so that I can answer any question you have about the proposal. Thank you.

Regards,

Michel

From: Michel Cukier
Sent: Monday, May 11, 2015 11:27 AM
To: Rama Chellappa
Cc: Michel Cukier
Subject: ACES (Advanced Cybersecurity Experience for Students) Minor Proposal

Dear Dr. Chellappa:

The purpose of this email is to obtain the approval to list the following classes, ENEE459C, ENEE459D, ENEE459E, as substitutes for one or two courses of the ACES minor.

Please find attached the proposal of the ACES minor. Pages 6-7 list the courses included in the proposed minor. We would like to list ENEE459C, ENEE459D, ENEE459E as substitutes for one or two courses of the ACES minor. We do not anticipate more students taking these classes due to the listing as substitutes in the ACES minor. Could you please confirm that you allow us to list ENEE459C, ENEE459D, ENEE459E as substitutes for one or two courses of the ACES minor.

Thank you in advance.
Regards,

Michel

---

Michel Cukier  
Director, Advanced Cybersecurity Experience for Students (ACES)  
Associate Director for Education, Maryland Cybersecurity Center (MC2)  
Associate Professor, Reliability Engineering  
Department of Mechanical Engineering  
University of Maryland  
3419 A.V. Williams Building  
College Park, MD 20742  
Phone: 301-314-2804  
Email: mcukier@umd.edu  
URL: http://ierpconnect.umd.edu/~mcukier/
Addendum to Senate PCC Proposal 15005: Proposal to Establish a Minor in Advanced Cybersecurity Experience for Students

Below are answers to additional questions raised about this proposed minor.

1) **Relationship of Minor Program to CMNS and ENGR.** Do the deans for CMNS and ENGR need to sign off on this proposal?

The ACES program is housed in the Honors College within UGST and was conceived as a multidisciplinary cybersecurity program. Note that CMNS has its own more technically focused concentration in cybersecurity. The ACES citation program recruits and compensates faculty from several colleges/schools on campus (BMGT, PUAF, BSOS, ENGR, CMNS) as well as from NSA and other organizations, and does not rely on the resources or facilities of these other programs. Deans Banavar and Pines were given copies of the proposal but requiring their sign-off seemed an unnecessary burden given that the ACES minor program draws few/no resources from them.

2) **Outside funding for this proposal.** The curriculum may move forward with the understanding that delivery is dependent on funding and that those conversations are ongoing, but the PCC needs better understanding of the funding stands.

The most recent update from the development staff is that Northrop Grumman plans to fund the ACES minor but has another internal meeting in early September and will make a commitment regarding the amount at or soon after that meeting. The ACES director and development staff have met regarding other funding sources, but one problem in seeking alternative funding is the uncertain status of the ACES minor—that is, it’s difficult to sell a program that does not yet formally exist.

3) **Instruction.** The Senate PCC will want to understand who is going to teach in the program, since neither UGST nor the Honors College have their own faculty.

One important feature of the ACES minor is the involvement of cybersecurity experts for teaching classes allowing the students to be up to speed with current trends in cybersecurity. NSA is currently teaching 2 classes for ACES (Reverse Engineering and the Puzzle class) and has offered to teach an additional 1-2 classes. MITRE also offered to teach one course in Spring 2016. We have also reached out to Northrop Grumman to provide one instructor a semester. Finally, the ACES renewal submission to Northrop Grumman includes funding for a full time lecturer.

4) **Admission.** The proposal says that the minor will be open to students outside the Honors College. Testudo indicates that HACS 402 is open only to students in the Honors College. Also, on p 1, there is the statement "...students will be admitted using Honors College admissions criteria". What does this mean?

ACES program leadership has worked closely with the Honors College (Bill Dorland and Traci Dula) to align the ACES minor admission criteria with criteria used by the Honors College (for example, the program does not rely solely on grades to make a determination but considers the complete application package). The current ACES minor admission process was approved by the Honors College and will require students to meet Honors College criteria, which has been defined on the website [http://www.aces.umd.edu/aces2/admission](http://www.aces.umd.edu/aces2/admission) as: minimum of 30 university credits/sophomore standing; minimum GPA of 3.0; and 4 semesters remaining at UMD prior to graduation. ACES program
leadership also recommend completion of one or more of the following with a B grade or higher: Calculus I, Introductory Statistics, Object-Oriented Programming, and Introduction to Engineering Design. With regard to Testudo, the restriction for HACS402 was worded erroneously in the provisional approval online form. It has been updated for permanent approval to state “must be a student in the ACES minor program.”

5) **Curriculum.** The proposal states that the program consists of 9 credits of upper level coursework (HACS 402, 404, 408, or authorized substitutes). It would be good to know what "authorized substitutes" means.

The “authorized substitutes” are listed in the table on page 7 of the proposal: “Students may also substitute 1 or 2 of the following 400-level courses: CCJS418B, CMSC414, CMSC456, CMSC498B, CMSC498R, ENEE459C, ENEE459D, ENEE459E, ENME442.” Note that there are emails with approval from department chairs or associate deans associated with these areas in the proposal.

6) **Libraries.** It would be good to have an email from the Libraries confirming the statement about library resources.

Please see the attached letter from the Libraries.
Michel Cukier, Ph.D.
Director, Advanced Cybersecurity Experience for Students
Associate Director for Education, Maryland Cybersecurity Center
Associate Professor, Reliability Engineering
Department of Mechanical Engineering
University of Maryland
3419 A.V. Williams Building
College Park, MD 20742

29 August 2015

Dear Dr. Cukier:

The University of Maryland Libraries provide this assessment in response to the proposal to offer an undergraduate minor in Advanced Cybersecurity Experience for Students (ACES). You asked that we assess our collections to determine how well the Libraries will be able support the curriculum of this proposed minor. We offer the following assessment, and conclude that the Libraries are able to support this program.

**Serial Publications and Research Databases**

In this technology-focused interdisciplinary field, curricular assignments and scholarly library research will rely primarily upon online serial publications. The University of Maryland Libraries currently subscribe to a large number of scholarly journals, almost all in online format, that publish current research in cybersecurity. Most articles in journals that we do not own are available through either the Libraries’ Article Express Program or via Interlibrary Loan. The Libraries’ “Database Finder” and “Research Port” offer online access to databases that provide indexing and access to scholarly journal articles and other information sources. Many of these databases cover subject areas that would be relevant to this proposed program. Most of the relevant technology-focused research is available through the following databases to which the Libraries subscribe:

- IEEE
- ACM Digital Library
- INSPEC
- Compendex

In addition, the following databases support research in the public policy and legal aspects of cybersecurity:

- Digital National Security Archive (DNSA)
- Lexis Nexis
- PAIS International

Also two general, multidisciplinary databases, *Academic Search Premier* and *MasterFILE Premier*, are good sources of articles relevant to this topic. In most cases, these indexes offer full text digital copies of the relevant journal articles. As noted previously, in those instances in which either the Libraries do not subscribe to the journal or the journal articles are available only in print format, the Libraries can supply copies through the Libraries’ Article Express Program or via Interlibrary Loan.
Monographs

Even though most library research for this course likely will rely upon online journal articles, students may wish to supplement this research with monograph materials. In many cases, relevant monographs will be available electronically as our book collections are increasingly available in electronic rather than print format. Even in instances when the books are only available in print, the students will be able to take some advantage of the book collection by requesting specific chapters be sent to them through the Libraries’ Article Express program. Faculty can also request, within fair use copyright guidelines, that sections of print books be made available digitally through course reserves.

Article Express and Interlibrary Loan

These services offer online delivery of bibliographic materials that otherwise would not be available online. As a result, remote users who take online courses may find these services to be quite helpful. Article Express and Interlibrary Loan are available free of charge. As a program developed specifically to support advanced research and teaching for graduate students and faculty, the Article Express service scans and delivers journal articles and book chapters within three business days of the student’s request, provided that the items are available in print on the UM Libraries’ shelves. In the event that an article or chapter is not available on campus, Article Express will automatically refer the request to Interlibrary Loan (ILL). Interlibrary Loan is a service that enables borrowers to obtain online articles and book chapters from materials not held in the University System of Maryland.

Student Services in the Libraries

The Libraries offer several programs that support student success. Subject specialists will provide students and other users with research support through individual consultation. Since this is an interdisciplinary program, librarians who work with collections and services for computer science, engineering, law, public policy and other areas will all be available for student assistance. The Libraries’ Research Commons offer students mentoring in research methodologies, writing assistance, statistical consulting, and other services.

Conclusion

The University of Maryland Libraries’ serial holdings and research databases have an established record for providing bibliographic support for researchers and professionals in subject disciplines that are relevant to cybersecurity. These materials are supplemented by relevant monograph collections. In addition, the Libraries’ Article Express and Interlibrary Loan services make materials that otherwise would not be available online, accessible to remote users in online courses. The Libraries also offer students a wide range of services to ensure their success. As a result, our assessment is that the University of Maryland Libraries are able to meet the curricular and research needs of the proposed Advanced Cybersecurity Experience for Students undergraduate minor.

Sincerely,

Daniel C. Mack
Associate Dean, Collection Strategies and Services