Proposal to Establish the ECS CENTER FOR CYBERSECURITY in the College of Engineering & Computer Science at CSUF

Executive Summary

Proposed Center Name:

Center for Cybersecurity in Engineering & Computer Science

Proposing Faculty Sponsors: (include departmental affiliations)

Mikhail I. Gofman (Department of Computer Science)
Shawn Wang (Department of Computer Science)
Yun Tian (Department of Computer Science)
Sinjini Mitra (Department of Information and Decision Sciences)

Mission and Purpose:

Introduction: Cyberattacks are on the rise. In the recent decades the cyberthreat landscape has evolved from hacker enthusiasts breaching systems for enjoyment to highly organized networks distributing malicious software for profit, large hacktivist groups working to undermine everyday operations of organizations, and government funded efforts to launch cyberattacks of remarkable levels of sophistication and destructive power.

Nobody is excluded; businesses, government institutions, and individuals are all potential targets.

Recent years have witnessed thousands of security breaches which highlight the growing prowess of modern cyberattackers. Some of the more notorious examples include:

● **Hacking of Anthem Insurance systems (2015)[1]** resulted in attackers gaining access to Social Security numbers and other sensitive data of millions of consumers and company employees.

● **Security breach of SONY systems (2014)[2]** resulted in the theft of several unreleased movies and terabytes of sensitive company data.

● **Infection of the Target store computers with malware (2013)[3]** allowed attackers to steal every credit card number used at the cash register. Overall, an estimate of 110 million credit and debit card numbers was stolen.

● **Attacks against J.C. Penney, 7-Eleven and JetBlue, and other companies (2013)[4]** resulted in the theft of more than 160 million cards.

● **The Stuxnet attack (2010)**[5] used highly sophisticated tactics to disrupt the systems controlling nuclear centrifuges at the Iranian power plant. A fraction of centrifuges were destroyed.

● **Security breach of Heartland Payment Systems (2009)**[6] resulted in the theft of 130 million credit card numbers.

These alarming trends have ushered in a demand for highly skilled security practitioners in the workforce and have created a field ripe with opportunities for research and development.

Orthogonally to the growth of cybersecurity threats, we intend to grow and develop ECS's involvement in curriculum development, applied research, and community outreach in the area of cybersecurity.

Having developed capacity in the area, ECS is now in a unique position to take its accomplishments in cybersecurity to the next level by consolidating all of its security-related activities under the common umbrella of the *Center for Cybersecurity*. The center will serve as a hub of security-related activities in ECS and on campus. It will create opportunities for faculty and students to collaborate on cross-disciplinary applied research projects and to engage in curricular leadership in the area of cybersecurity. In addition, the center will also serve as a point of contact for both public and private sector industries interested in working with and/or hiring ECS students and collaborating on research projects.

The ultimate goal of the center will be to transform ECS into a national leader in security education and research.

Goals, objectives, and activities:

The broader goals of ECS Center for Cybersecurity can be summarized as: *education, research, and outreach in the area of cybersecurity*. In each of these areas the center will adopt a multipronged strategy geared toward maximizing the benefit for students, faculty, industry partners, and the broader community. The strategy can be broken down into the following specific objectives:

● **Security Education:** The center will work to train top-notch security practitioners and to introduce relevant security topics into security-related courses in ECS and campus-wide.

1. ***Establish and maintain a top-notch, interdisciplinary designed cybersecurity curriculum based on high-impact pedagogical practices and geared toward training the next generation of security practitioners.***

   The center will bring together faculty members from multiple disciplines, including computer science, various disciplines of engineering business and other related disciplines, to jointly work on developing and maintaining the cybersecurity curriculum based on high-impact pedagogical practices, applied knowledge, and multidisciplinary perspectives.

   The curriculum development will be steered by the following guiding principles:

a. Emphasis on high-impact pedagogical practices: Studies have confirmed that hands-on, project-based learning experiences lead to greater levels of mastery of the material[8]. Toward this goal, the curriculum shall emphasize project-based learning experiences, industry and government internships, hands-on design and implementation of security systems and protocols, participation in hacking and counter-hacking activities, writing and analysis of security requirements, and other high-impact learning practices.

b. Focus on applied knowledge: In the age where cyberattacks are an everyday occurrence, no organizations are safe without skilled, competent security practitioners on their staff or a trustworthy security consultant.

   The curriculum shall emphasize practical skills readily applicable in the workplace, including the use of state-of-the-art security technologies and methodologies, analysis of real-world security breaches, construction and analysis of threat models, and other applied security skills vital for success in the modern workplace.

c. Emphasis on multidisciplinary approach to curriculum design: Comprehensive solutions to the security problems of today and tomorrow must be technically sound, financially sustainable, must minimize negative social impacts (e.g., intrusion on people's privacy), and be subject to the highest ethical standards.

   For example, although cybersecurity is vital to the wellbeing of any organization, many managers and employees do not see cybersecurity as a tangible benefit; security is often viewed as an obstacle to convenience, an excuse for infringing on privacy, and an added financial burden with little return of investment. How should a security professional working for a company convince the employees to cooperate with security policies and convince management to invest in security? Answering these questions requires not only strong technical skills, but also familiarity with business management, psychology, and finance.

   For these reasons and more, the curriculum shall incorporate perspectives from multiple disciplines, including computer science, engineering, business, and psychology, geared toward giving students a richer understanding of problems of security. Faculty from the department of Information and Decision Sciences at Mihaylo College of Business and Economics and faculty from Computer, Mechanical, and Civil Engineering departments at ECS have already expressed interest in contributing to these efforts (please see sample email attached).

   In addition, throughout the curriculum development process, feedback from industry and government will play an integral role in shaping the curriculum.

   Finally, because teaching cybersecurity routinely requires the use of information technology, the expertise of the campus Information Technology (IT) department will be utilized to help evaluate new use cases of campus IT resources.

One of long-term objectives of the curriculum development activities of the center will be to transform ECS into a National Security Agency (NSA) recognized *National Center of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD).* The Computer Science department at ECS has already taken steps toward fulfilling this goal.

Another goal of the center will be to enrich the courses the Computer Science department currently offers in introductory cybersecurity, cryptography, network security, and cloud computing security, with relevant perspectives from computer engineering and business disciplines and to use industry feedback to revise courses in ways that maximize student success in the workplace.

The center will also work to develop more security courses. Development of other security courses is already underway in the Computer Science department and may be pursued more vigorously with the establishment of the center.

2. Promote awareness of cybersecurity issues in non-security courses and disciplines.

Many security breaches occur as a consequence of actions of professionals or users in disciplines other than cybersecurity. For this reason, it is critical for professionals of all areas, especially those in technical fields, to comprehend the fundamentals of cybersecurity.

The center will work to ensure that *all* students get the necessary exposure to cybersecurity. This includes incorporating the introductory course in cybersecurity into the core computer science curriculum and ensuring that all courses in the Computer Science department, engineering departments in ECS, and other departments across campus teach relevant cybersecurity concepts in their related courses.

- **Security Research:** The center will pursue two key research objectives: create opportunities for undergraduate and graduate students to engage in project-based learning experiences and to develop novel research funded by external grant proposals.

1. Engage undergraduate and graduate students in project-based learning experiences through involvement in security research projects.

Project-based learning is a high-impact pedagogical practice that promotes learning and helps develop practical skills. The center will seek to engage students from ECS and other colleges on campus, in cybersecurity research projects hosted by the faculty.

We believe that ECS will be very successful in achieving this objective as ECS has a rich history of involving students in security research. This fact is highlighted in the following examples:

● Computer Science department faculty Dr. Mikhail I. Gofman jointly with Dr. Sinjini Mitra from Department of Information Systems and Decision Sciences at Mihaylo college, have created an informal biometrics research group which currently involves four undergraduate and four graduate students. In the Fall of 2014 semester, students presented their work at *The Southern California Conference for Undergraduate Research* and one student won an *Outstanding Scholarly and Creative Activities Award* in 2015. The students have also authored papers to peer-reviewed conferences and journals (including the Communications of ACM).

Dr. Gofman has also headed a group of students working on system security research. In the Fall 2013 semester, one of Dr. Gofman's graduate students co-authored a journal paper which proposes a solution to the problem of securing virtual machine checkpoints. The paper was accepted to a highly competitive, peer-reviewed journal (*Special Issue on Information Assurance and System Security in Cloud Computing, Journal of Cloud Computing*).

● Dr. Yun Tian from the Computer Science department currently heads a cloud computing & security and big data research group. The group involves 5 graduate students and 3 undergraduate students. In the summer of 2014, students presented their work at STEM Summer Research Symposium.

Dr. Tian also works in the field of social computing. In May 2014, one of her graduate students co-authored a poster paper and presented it in the 2014 *ASE BIGDATA/SOCIALCOM/CYBERSECURITY* Conference at Stanford University.

● Dr. Shawn Wang from the Computer Science department published two papers to peer-reviewed conferences, with students being the primary authors. The papers proposed novel solutions to problems in areas of network security and cryptography.

● Dr. Kevin Wortman from the Computer Science advised several student projects related to security. One of the projects focused on the use of biometric data (e.g., muscle movement) for generating cryptographic keys used for protecting data from unauthorized access.

2. Foster initiatives for conducting cybersecurity research and developing research grant proposals.

The center will engage in activities incentivizing faculty to produce research publishable in peer-review journals and develop research grant proposals. Using the language of National Science Foundation proposal solicitation, the Center for Cybersecurity will provide a "Center-based [research] environment in which the whole is greater than the sum of its parts"[7].

Potential incentives may include (but are not restricted to) allowing faculty with security research projects promising to result in publications to high ranking security venues, to apply for center grants. The center will also support faculty interested in developing security-related grant proposals in attending training workshops. Finally, the center plans to recognize faculty and students for the following categories at an awards event:

- Faculty with superior research publication records.
- Faculty who were able to procure significant extra-mural funds for security-related research projects.
- Students with outstanding track records of undergraduate or graduate cybersecurity research.

In addition, multiple ECS faculty are currently actively engaged in writing grant proposals in areas of cloud computing security, big data security, network and system security, mobile device security, biometrics, access control, and hardware security.

Some examples of current activities include:

- Dr. Mikhail I. Gofman in the Computer Science department is currently researching approaches for protecting mobile devices from unauthorized access using biometrics (i.e. identifying people using their physical traits and behavioral characteristics). This is inter-disciplinary work with Dr. Sinjini Mitra from Department of Information Systems and Decision Sciences at Mihaylo College. The project was recently awarded Intramural, Incentive, and Faculty Mentorship of Undergraduate Research and Creative Activities grants. Dr. Gofman and Dr. Mitra are in the process of using the funds to develop a National Science Foundation (NSF) *Secure and Trustworthy Cyberspace (SaTC*) grant and *Google Faculty Awards* grant proposals to fund their research.

- Drs. Binod Tiwari[CE], David Naish[CE] , Phoolendra Mishra[CE], John (Kenneth) Faller[CpE], Yun Tian[CS], Mikhail Gofman[CS], Joseph Piacenza[ME], and James Miller[GEOG], have submitted a grant proposal to the NSF Science, Engineering and Education for Sustainability (SEES) program. The grant develops a new system for predicting earthquake induced mudslides which plague many locations in the world. On the of the integral components of the proposed system is a cybersecurity subsystem which helps secure the wireless sensors used for instrumenting mountain slopes.

CE	Department of Civil and Environmental Engineering
CpE	Department of Computer Engineering
CS	Department of Computer Science
ME	Department of Mechanical Engineering
GEOG	Department of Geography

- Dr. Yun Tian in the Computer Science department is currently researching approaches for making cloud systems more resistant and resilient against attacks, with plans of writing grant proposals in the near future.

  Dr. Mikhail Gofman is researching approaches for making virtual machine checkpointing, an approach widely used for backing up data in cloud computing systems, more secure from attackers who have gained access to checkpoint files. Gofman is also researching solutions to security problems in access control systems and operating systems.

  The Center will work to bring these faculty together as well as seek to involve faculty from other departments and schools to jointly work on authoring peer-reviewed publications and white papers and developing grant proposals.

● **Security outreach:** the center will host public events and workshops aimed at educating industry professionals and the broader community in the fundamentals of cybersecurity, will work to forge ties with industry in order to attract funding necessary for supporting center activities, and will cooperate with industry on addressing real-world security issues.

1. To host professional development events aimed at educating non-security professionals and the broader community in the fundamentals of cybersecurity.

Cyberattackers target everybody. A weak password of a single user can become a potential security breach point. Now more than ever, it is critical for professionals of all areas as well as individuals understand the importance of properly securing their assets, products, and services, against the actions of cybercriminals.

Toward the above-stated goal, the center will hold workshops, symposia, and keynotes aimed at educating the professionals and the public about cyberthreats and cyberthreat countermeasures. The center will also engage in activities geared toward countering the popular sentiment that security is simply a barrier to convenience, an excuse for infringing upon the privacy of individuals, and a low priority item on the list of things the organization needs to invest in.

ECS has already successfully experimented with the idea of hosting security-themed public events. In Fall 2013 and Fall 2014 semesters, ECS held the *Security Day Event* which featured talks by security professionals from both public and private sector industries as well as by the Computer Science department faculty. In both years, the events were well attended and were widely praised by the attendees.

2. Engage with industry to attract funding for sponsoring security-related center activities.

CSUF is strategically located in a business district where major industry players, including Raytheon, Boeing, Deloitte, Northrop Grumman, and many other companies have a strong presence.

ECS has a longstanding strategic partnership with Raytheon, Broadcom, Cisco, Disney, Emulex, Experian, Facebook, Google, IBM, Linksys, Thales Group, Unisys, and Western Digital corporations.

Raytheon has funded security-related outreach events at ECS, facility improvements, and student activities such as hackathons. Using Raytheon partnership as a model, the center will reach out to other companies and government institutions interested in security.

3. Help industry partners solve security problems.

ECS employs cybersecurity faculty with capacity and desire to help our industry partners resolve their security issues.

The center will serve as the point of contact to foster partnership between faculty and industries interested in addressing security problems.

Location

The Center will be housed in the College of Engineering and Computer Science.

Membership

The center shall welcome all faculty interested in contributing to the curriculum development, research, and outreach goals of the center, students interested in working on specific center projects, and external entities (which include but are not limited to representatives from industry, academia, and government) interested in making a specific contribution to the center goals.

All faculty members working on the center curriculum development, research, and outreach activities shall have the title of the center *Associates*.

All students affiliated with the center shall have the title of the center *Fellows*.

All external parties (e.g. companies from industry) working with the center shall have the title of the center *Partners*.

Bylaws

The center administrative structure shall comprise the center director, three assistant directors, and external advisory board. Each of the three assistant directors shall be responsible for coordinating curriculum development, research and grants acquisition, and outreach activities of the center, respectively. The director shall have the duty of overseeing, granting activity approvals to the assistant directors, proposing center activities, maintaining an external advisory board composed of representatives from cybersecurity field not affiliated with CSUF, and approving membership of prospective center associates, fellows, and partners.

The privileges and duties of the director, assistant directors, and the advisory board can be summarized as follows:

- **Director:**

  a. The director shall be appointed by the Dean of the ECS and shall serve a three year term which can be renewed upon the recommendation of the Dean.

  b. The director shall oversee all center curriculum development, research and grant acquisition, and outreach activities and delegate the tasks of coordinating these activities to the appropriate assistant directors. Throughout the process the director shall maintain an active involvement in ensuring the success of all activities.

  c. Every semester the director shall prepare a detailed report outlining the curriculum development, research and grant acquisition, and outreach activities undertaken by the center, as well as detailing the initiatives, goals, and plans the center plans to pursue in the coming semester.

  d. It is the responsibility of the director to ensure that all executive positions of the center remain filled by seeking the willing and qualified candidates and recommending them to the Dean of the ECS for approval.

  e. The director shall meet regularly with the assistant directors in order to discuss the status of ongoing center activities and give approvals for new activities.

  f. The director shall work with assistant director of research and grant acquisition to develop grant proposals targeted toward funding the center.

  g. The director shall be the point of contact for all matters concerning the center, which includes interviewing prospective associates, fellows, and partners interested in joining the center and approving the center memberships.

h. The director shall maintain a board consisting of 5-10 security professionals and professionals from related fields from outside of CSUF. The director shall appoint members every semester and have these members approved by the Dean of the ECS.

   The director shall meet with the board each semester and solicit feedback on curriculum development, research, and outreach activities of the center. The director shall then present and discuss the recommendations of the board to the assistant directors or require assistant directors to attend the board briefings.

- **Assistant Director of Curriculum Development:** the roles and responsibilities of the assistant director of curriculum development can be summarized as follows:

  a. The assistant director of curriculum development shall be charged with the duty of advancing the center curriculum development objectives, which includes organizing inter-disciplinary committees of associates for the goals of designing security course proposals, integrating security into existing courses, designing new, innovative ways of teaching security, and tackling all issues concerning curriculum development.

     During all meetings the assistant director shall take meeting minutes and submit them to the director.

  b. The assistant director of curriculum development shall work closely with the director toward allowing the CSUF campus to be recognized by the National Security Agency's criteria for recognition as the National Center of *Academic Excellence in Information Assurance (IA)/Cyber Defense (CD).* Once this objective has been accomplished, the assistant director shall work to ensure that the campus maintains the status.

  c. The assistant director shall meet regularly with the center director to report the status of the ongoing curriculum development activities and receive director's approval for prior to commencing new curriculum development activities.

  d. At the conclusion of each semester, the assistant director shall prepare a report documenting all center curriculum development activities undertaken by the center that semester and curriculum activities planned for the upcoming semester. For each curriculum development activity, the report shall include the following details:

     - A summary of the curriculum development activity.
     - The current status of the activity.
     - The detailed summary of the center budget expended in executing the activity (if applicable).
     - The next steps of the activity.
     - Curriculum development activities planned for the next semester.

The report shall also highlight any important miscellaneous information regarding center curriculum development activities.

e. The assistant director shall keep the curriculum development portion of the center website up to date with latest information regarding the center's curriculum development activities and accomplishments.

- **Assistant Director of Research and Grants:** the roles and responsibilities of the director can be summarized as follows:

  a. The assistant director shall be charged with the duty of advancing the research goals of the center as well as spearheading the process of preparing grant proposals for funding the center activities. Specifically, the assistant director of research shall organize committees of faculty (i.e., center associates) and students (i.e., center fellows) to work on security research projects and prepare research grant proposals. During committee meetings, the assistant director shall keep meeting minutes. The meeting minutes must be reported to the center director promptly after the conclusion of the meeting.

  b. The assistant director jointly with the director shall have the responsibility of vetting the prospective center associates interested in joining the center for the purpose of conducting research or developing proposals.

  c. The assistant director jointly with director shall have the responsibility in seeking out and working on grant applications necessary to procure funds for supporting the center.

  d. The assistant director shall have the responsibility of assigning prospective center associates, fellows, and partners to ongoing research project activities and shall have the power to dismiss fellows from projects.

  e. The assistant director shall meet regularly with the center director to report the status of the ongoing research and grant writing activities and receive director's approval prior to commencing new research activities.

  f. Upon the conclusion of each semester, the assistant director shall prepare a report documenting all research and grant acquisition activities undertaken by the center that semester and activities planned for the upcoming semester. For each research activity, the report shall include the following details:

     - A summary of the research activity.
     - Will the activity result in publication of peer-reviewed works to conferences, journals, workshops, etc.? If so, then to what venue and at what date will/was the manuscript be submitted?
     - Center members involved in the activity.
     - The current status of the activity.

- The detailed summary of the center budget expended in executing the activity (if applicable).
- The next steps of the activity.
- Research activities planned for the next semester.

For each grant proposal writing activity the report shall include the following details:

- A summary of the grant proposal.
- The status of the proposal.
- Center members involved in writing the proposal.
- The amount of the grant.
- The funding agency.
- The center budgets expended in preparing then proposal.

In addition, the report shall include a summary of all accepted peer-reviewed publications and grant proposals.

g. The assistant director shall maintain the center webpage documenting all accepted peer-reviewed publications and funded grant proposals.

- **Assistant Director of Outreach:** the roles and responsibilities of the director can be summarized as follows:

a. The assistant director of outreach shall be charged with the duty of coordinating all center activities pertaining the center's outreach to CSUF, industry, government, community, etc.

b. The assistant director shall be charged with the responsibility of planning and holding the *ECS Security Day* event every fall semester.

c. The assistant director shall organize activities designed to educate the general public on cybersecurity issues.

d. The assistant director shall work to connect with industry, government, academic institutions, and individuals in order to inform them of the center activities and solicit financial support for the center.

e. The assistant director shall create committees consisting of center associates, fellows, and partners necessary for executing community outreach activities. The assistant director shall hold meetings with the committees and keep meeting minutes. The meeting minutes must be reported to the center director promptly after the conclusion of the meeting.

f. The assistant director shall meet regularly with the center director to report the status of the ongoing outreach activities, receive director's approval prior to commencing new outreach activities.

g. At the conclusion of each semester, the assistant director shall prepare a report documenting all outreach activities undertaken by the center that semester and activities planned for the upcoming semester. For each research activity, the report shall include the following details:

    - A summary of the outreach activity.
    - Targeted groups (e.g. industry, general public, etc).
    - Center members involved in the activity.
    - The current status of the activity.
    - The detailed summary of the budget expended in executing the activity (if applicable).
    - The next steps of the activity.
    - Outreach activities planned for the next semester.

h. The assistant director shall maintain the center webpage announcing the center outreach events.

- **The Advisory Board:** The advisory board shall consist of 5-10 security professionals from industry, government, and other academic institutions not affiliated with CSUF. The board members shall be appointed by the director and approved by the Dean of ECS and shall meet once a semester with the director in order to provide feedback on the center curriculum development, research, and outreach activities. Initially, the center shall reach out to the following institutions in order to recruit board members:

    - Raytheon, Boeing, Deloitte, Bechtel, Cigital, E2VE and Northrop Grumman corporations
    - Sandia National Labs
    - State University of New York at Binghamton
    - University of Houston-Clear Lake
    - **<u>Revision of Bylaws</u>**

Revision of bylaws: The bylaws shall be reviewed and may be revised every year by the director and the assistant directors. The revised by-laws must be approved by the Dean of the ECS prior to going into effect.

Fiscal Policies

- The fiscal year shall correspond to that of CSUF.

- The books and accounts of the center shall be kept by CSUF and shall be audited in accordance with CSUF policies.

- The center budget shall be derived from external funding sources and ad-hoc support from ECS funds and shall be administered by the center director and approved by the Dean of the ECS.

Involved Departments and/or Colleges:

The center will initially involve members from Computer Science, Computer Engineering, Electrical, and Civil Engineering departments and members from Department of Information Systems and Decision Sciences at Mihaylo College.

Any colleges and departments interested in contributing to the mission and goals of the center shall be welcome to join the center and participate in the center activities.

Short- and Long-term Plans:

The short-term and long-term goals of the center can be summarized as follows:

Curriculum Development:

1. Identify parts of the Computer Science department security curriculum that are deficient in high-impact pedagogical practices and work on addressing the deficiencies.

2. Identify non-security courses in the Computer Science department curriculum where relevant security concepts should be taught.

3. Make faculty search committees in the ECS aware of the need to recruit faculty with expertise in cybersecurity.

4. Establish synergistic ties with engineering departments at ECS and other departments on campus and develop a process for multidisciplinary approach to curriculum design and development.

Research:

1. Reach out to ECS faculty and to faculty in other colleges to identify opportunities for collaborative research and grant proposal writing.

2. Develop a formal process for identifying and recruiting students interested and qualified to work on the center-sponsored research projects.

3. Identify the immediate benefits which the center can deliver to the presently ongoing grant proposal writing activities.

Outreach:

1. Plan for Security Day event in Fall 2015 semester.

2. Identify the type of professional development events which the center plans to hold in the future and plan their high-level logistics.

3. Establish a plan for making the center presence known on and off campus.

The long-term goals of the center can be summarized as follows:

Teaching:

1. Integrate the course in introductory cybersecurity into the core curriculum of the Computer Science department.

2. Develop a security curriculum in the Computer Science department which fulfills the National Security Agency's criteria for recognition as the *National Center of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD)*.

3. Develop undergraduate and graduate advising tracks in cybersecurity in the Computer Science Department targeted at producing highly trained security practitioners and work on establishing similar tracks at other departments at ECS.

4. Establish standing committees consisting of ECS security faculty and faculty from other departments, in charge of developing and revising the security curricula at ECS and other colleges.

5. Develop a formal process for soliciting feedback on the security curricula from industry and establish a working relationship with the Information Technology department for testing novel use cases of information technology in teaching cybersecurity.

Research:

1. Develop a formal process by which a faculty member with a research idea or an initiative to develop a grant proposal can use the center as means of recruiting collaborators and co-PIs.

2. Develop a formal process by which the center will connect faculty with students qualified to participate in project-based learning experiences.

3. Establish a community of faculty and student scholars which jointly works together on applied research resulting in peer-reviewed publications and grant proposals.

Outreach:

1. Make the center the point of contact for representatives of public and private sectors interested in providing internship opportunities for students, recruiting skilled security practitioners, working on joint research projects with faculty, and sponsoring security-related activities at CSUF.

2. Establish a yearly schedule of security outreach events such as *Security Day* and professional development workshops.

3. Establish the center as the academia to industry pipeline for students interested in pursuing cybersecurity careers.

Budget, Personnel and Space Requirements:

The annual budget requirements of the center are outlined below. The salient budget items include a student assistant to perform secretarial duties at the center office and space where students involved with center activities will work. These items may change as the center evolves.

Room CS-106 (see photo below) in the Computer Science building was already allotted by the Office of the Dean to house all students interested in participating in center projects.

Room CS-410 (see the photo below) in the Computer Science building was allotted by the Computer Science Department to house students and research equipment and to accommodate center growth and expansion.

Room CS-106	**Room CS-410**

The center shall require a $30,000 per year budget. An estimated budget breakdown is given below:

Budget Breakdown:

Phase 1	**Initiation period**	
	Tasks: Identify internal partners, identify space, prepare a vision plan, recruit graduate students for exploratory work, get internal approval	
	Salary, Center Director	$ 12,000.00
	Salary of a student assistant to perform secretarial duties at the center office	$ 20,000.00
	Holding the annual Security Day Event	$ 3,000.00
	Holding professional development workshops, conferences, and symposia	$ 5,000.00
	Purchasing computing equipment and similar resources necessary for research	$ 10,000.00
	Education, research, and outreach related traveling expenses for center members	$ 5,000.00
Phase 2	**Regional and national promotion**	
	Attend workshops and conferences	
	Prepare grant proposals from national federal agencies	
	Identify private industries and private funding sources as well as prepare proposals	
	Federal grants	$ 500,000.00
	Private foundation grants	$ 200,000.00
	Internal support	$ 10,000.00
	Secretarial support	$ 20,000.00
Phase 3	**Steady state**	
	Research funding	$400,000-$600,000 annually

Compensation for duties of assistant directors shall be provided by their respective departments or colleges.

Specialized Equipment Requirements:

As the center grows and expands, various computational equipment and software may be necessary for training and research. The specifics of the equipment will depend on the specific educational and research projects in which the center will be involved in in the future. We intend to gather external support either from the industry or grant agencies to eventually build new facilities.

Catalog Description: The *Center for Cybersecurity* in the College of Engineering and Computer Science at CSUF engages in educational, research, and outreach activities in the area of cybersecurity.

References:

1. Finkle, Jim. "'U.S. states say Anthem too slow to inform customers of breach". *www.reuters.com*. February 11, 2015. Web. February 11, 2015. <http://www.reuters.com/article/2015/02/11/us-anthem-cybersecurity-states-idUSKBN0LE2QP20150211>

2. "'Sony-pocalypse': Why the Sony hack is one of the worst hacks ever". *CNN.com*. December 29, 2014. Web. February 3, 2015. <http://money.cnn.com/2014/12/04/technology/security/sony-hack/>

3. "Target breach: How things stand". *CNN.com*. May 5, 2014. Web. Web. February 3, 2015.

4. Jones, David and Finkle, Jim. "U.S. indicts hackers in biggest cyber fraud case in history". *Reuters Press*. July 25, 2013. Web. February 3, 2015. <http://www.reuters.com/article/2013/07/25/us-usa-hackers-creditcards-idUSBRE96O0RI20130725>

5. Langer, Ralph. "To Kill a Centrifuge." *The Langner Group*. November 2013.

6. Zetter, Kim. "The 10 Biggest Bank Card Hacks". *Wired.com.* December 2, 2014. Web. February 3, 2015. <http://www.wired.com/2014/12/top-ten-card-breaches/>

7. "The 6 Elements of High Quality Practices." *fullerton.edu*. Web. February 3, 2015. <http://www.fullerton.edu/cice/Faculty_HIPteaching.html>

8. "Science and Technology Centers: Integrative Partnerships." *National Science Foundation*. 2014. Web February 4, 2015. <http://www.nsf.gov/pubs/2014/nsf14600/nsf14600.htm>