Motion: that Faculty Senate approve the creation of a new center, the Cybersecurity and Cyberdefense Policy Center.

****

May 27, 2022
To: Faculty Senate Steering Committee
From: Educational Policy Committee (EPC)
Re: Cybersecurity and Cyberdefense Policy Center Proposal

The EPC met and reviewed the proposal for the Cybersecurity and Cyberdefense Policy Center on May 20, 2022. There was consensus of general support for the center as written. EPC recognized the funding source as historically consistent and the focus of the center as relevant and urgent in today's world. Although there is no PSU policy or expectation, EPC wants to encourage those starting this center to have a contingency plan should an unfortunate and/or unexpected loss of the current funding occur.

EPC also wants to acknowledge the context of discussing funding for a new center while simultaneously programs within the school and university are undergoing scrutiny, pressure and threats of cuts. This is both to acknowledge the stress faculty and staff are experiencing and emphasize the already noted need from the Budget Committee for this center to be mindful of sustainable funding outside of the school and university. This is part of the reason EPC is strongly encouraging those developing this center to look at internal existing resources, programs and centers for collaboration. EPC sees this center as having great potential to partner and collaborate with existing entities on campus to strengthen the university community across silos.

EPC thanks the developers of this proposal and supports the implementation of this center.

Creation of an Academic Unit

1. Identify the type of unit (see accompanying approval process flow chart and description for each):
    a. College: **CUPA**
    b. School: **Mark O. Hatfield School of Government**
    c. Academic Department: N/A
    d. Academic Program: N/A
    e. Research/Membership Center/Institute:
    Mark O. Hatfield Cybersecurity and Cyber Defense Policy Center ***(NOTE: Please note that all references to the Center's title below will be changed to Hatfield Cybersecurity & Cyber Defense Policy Center in the Diagrams).***
    f. General Support or Public Service Center/Institute: N/A
2. Proposed name of the unit?
Mark O. Hatfield Cybersecurity and Cyber Defense Policy Center

3. How does the unit help Portland State University to achieve its goals (e.g., pedagogy, research, community service, diversity and inclusion)?

Portland State University (PSU) has been designated a **National Center of Academic Excellence in Cyber Research** (NCAE-CR) by the National Security Agency (NSA) and the Department of Homeland Security (DHS). We are also an academic partner of the US Cyber command. PSU's excellence in Public Affairs education, workforce training, and community engagement in solving policy challenges, Computer Sciences and Engineering, and Business Administration presents a unique opportunity to build cross-disciplinary collaboration among faculty and students in the Cybersecurity and cyber defense fields. **The Mark O. Hatfield Center for Cybersecurity and Cyber Defense Policy will** be a collaborative partnership of PSU Colleges and Schools dedicated to bringing together scholars, industry partners, and policymakers to train a diverse group of students and translate research findings into effective policy for Cybersecurity and cyber policy defense. PSU faculty follow the university's motto, **"Let Knowledge Serve the City,"** to pursue scholarships in an applied setting. Our Center distinguishes itself from other NCAE-C Research centers by its niche research in local governments' cybersecurity and cyber defense. It emphasizes building **a bridge between technology (computer sciences and engineering), collaborative governance, public policy, and public awareness.** We will create a pipeline of diverse students in research projects through partnerships with the region's Community Colleges. Portland Community College, Mt. Hood Community College, and Chemeketa Community College are CAE-C 2-year institutions and have agreed to partner with us. This is an excellent opportunity to expand our research work and leverage it for more academic degree programs and non-credit certificate programs targeting workforce development.

There is a severe shortage of qualified professionals from diverse backgrounds in the cybersecurity field. Most people come from technical areas of academia. According to the US Cyber Command, echoed by industry executives, we need to train people in cross-disciplinary fields focusing on cybersecurity and cyber defense. Our research center will provide opportunities for interdisciplinary research opportunities for students and faculty. Bridging opportunities for Science, Technology, Engineering, Arts, and Mathematics (STEAM) fields of study and career paths for women and people of color has been a critical movement in the PNW Region over the last fifty years. In Cybersecurity, the lack of cultural representation creates national security risks - limited perspectives more quickly devolve into groupthink. There is an urgent need to build the pipeline from K-12 to employment through engaging hands-on experience, education, and training. Racial and ethnic diversity in the intelligence community enhances U.S. national security. Security and equity are paramount in addressing the complexity of soft and hard sciences needed to identify and decode cybercriminals' evolving agendas. By attracting women and people of color to Cybersecurity, our proposal creates a more secure network and the necessary tactical and operational workforce to defend our shared assets.

4. What are the objectives and planned outcomes for the unit?

There are several planned objectives and outcomes for the Center:

a. Attract research funding from the public and private sectors for interdisciplinary projects. As explained in the *White Paper* (see attached), our research group successfully raised a $3 million 3-year grant from the NCAE-C (in NSA) to research, analyze, and identify weaknesses in hardware and workforce in the Power Grid in the Pacific Northwest and pull together a Cybersecurity Critical Infrastructure Community of academic, private, and public partnership to address the needs of the region. This project employs graduate students and faculty from PSU and partner institutions in Oregon, Washington, Idaho, and Colorado.
b. We also received an appropriation of $600,000 from the US Congress for a cybersecurity education project. We will use these funds to hire faculty and staff for non-credit certificate programs for workforce development for local governments, to establish GenCyber programs for High School students during the Summer months (use the funds to obtain more funding from NSA and NSF for GenCyber), and invite our regional Community College partners to administer workforce training educational programs jointly. Finally, we will provide incentives for PSU faculty to develop courses in the cybersecurity field in various academic units that could be used in these workforce development programs.
c. Use the Center's research programs to enhance interdisciplinary educational programs across PSU to stay ahead of the competition in Oregon. The University of Oregon is planning to introduce a multidisciplinary BA degree in cybersecurity. This idea comes directly from the attached *White Paper,* shared with UO and OSU during the State Legislature's public hearing. We presented concepts for the Oregon-wide Cybersecurity Center of Excellence (led by PSU). The initiative did not come up for funding in February 2022, but the group was invited to reintroduce the concept for consideration in the 2023 budget.
d. We want to keep PSU's NCAE-C designation as the "go-to" place with this Center for research and development projects that focus on *America's Soft-Underbelly* (local governments, local public utilities, small

cooperatives, K12 Districts, Counties, Healthcare institutions). This requires a massive amount of coordination and collaboration between private and public sector stakeholders, which our Center can serve as the critical support unit. Having received the NSA's designation (only university in Oregon) and one of nine major grants in 2021, we are uniquely positioned to move ahead and secure more funding as private, and public institutions approach us for partnerships.

5. What significant activities will take place within the unit?
    a. Indicate the expected percentage of time and resources allocated to each activity. Please include, if appropriate: courses to be offered, course development, research performed, community partnerships built, and others (specify).

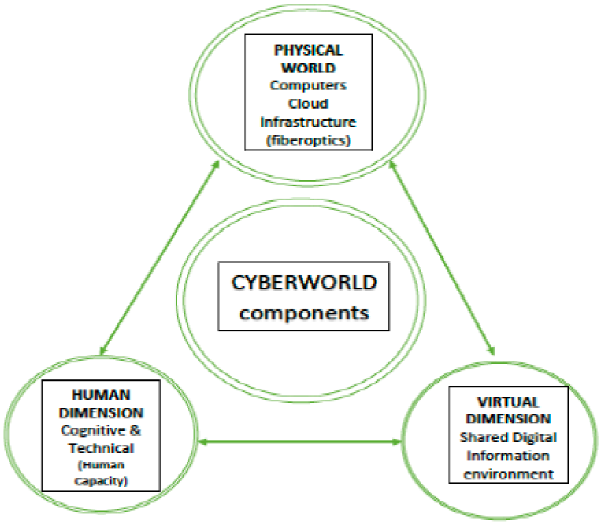
Our Center is primarily a research-based institution with non-credit certificate programs for workforce development for local governments. We will apply for research funding in cybersecurity and cyber defense from federal and private sources. Train students (undergraduate and graduate), hold public awareness programs such as webinars, public talks, and panel discussions, sponsor small workshops and conferences, publish proceedings, and publish research findings.

Community partnerships already in place include Oregon's Titan Fusion Center, FBI, NSA, CISA, DHS, Oregon Guard, the League of Oregon Cities, Association of Oregon Counties, K12 School Districts Association, Special Districts Association of Oregon, LinkOregon, Paloalto Networks, Pacific Northwest National Lab, BPA, PGE,

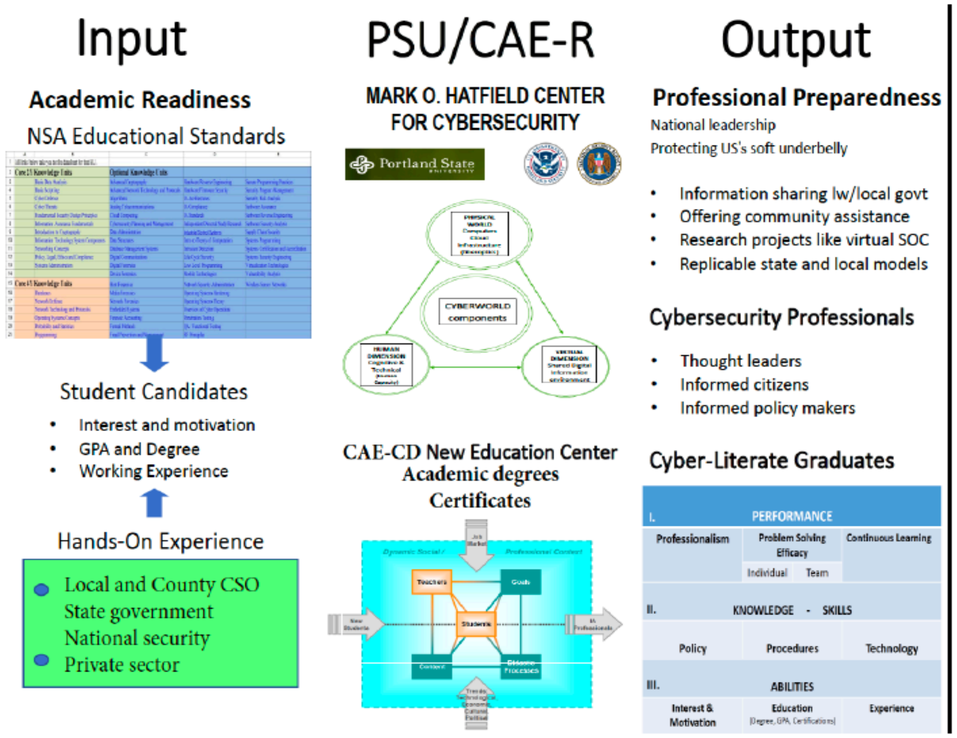
6. Why is a new unit needed to achieve these outcomes and host these activities?
    a. What other units are already undertaking similar activities? Meet with these units and include documentation on the outcomes of these meetings.
    b. Why is a separate identity and structure key to success in meeting the objectives and planned outcomes?
    c. How will these outcomes be measured and assessed? What benchmarks will be used to determine the success of the unit?

I will try to address these issues collectively. Until two years ago, there was no effort to coordinate cybersecurity initiatives at PSU. I realized the need for an inter-college and interdisciplinary need for research and development and multidisciplinary education during my discussions with national peer institutions representatives at a conference. This coincided with when former Dean of MCECS Rich Corsi was hired. I asked him for a meeting, and we agreed that there is a need between engineering and public policy in general and, more specifically, in the cybersecurity and cyber defense field for broader collaboration between engineering, social sciences, humanities, life sciences, business, mathematics, and public policy/political science. Provost Jeffords invited us to meet her former colleagues from UW-Bothell who were visiting PSU, and we discussed academic and national policy needs in these areas of cyber studies. Provost Jeffords then invited me to form a task force to engage faculty discussion across PSU in this area. After a year of meetings, we decided to apply for a Cybersecurity Research designation by the NSA and DHS to join the national network of 340 universities of colleges engaged in cybersecurity education programs and research activities. We also realized how rich PSU is in this area across at least four colleges: CLAS, MCECS, SB, and CUPA. We decided to apply for the research designation as a step in the right direction for increasing collaboration between our units and then pursue discipline-specific (i.e., Computer Science graduate certificate) and an interdisciplinary undergraduate degree and stackable certificates for graduate programs shortly. While we are working with the assistance of the Deans of our respective units and the Dean of the Graduate School, we need to establish our research center where all these interested faculty can be affiliated and participate in collaborative research projects. So, the Hatfield Cybersecurity Center will be the only research center focusing specifically on technical, policy, ethics, and other vital areas in cybersecurity and cyber defense. It will be truly interdisciplinary and provide educational training opportunities for students and directly benefit the university and its community partners. It will also give PSU the advantage over OSU and UO in this increasingly important field of academic innovation and policy prescription for public and private partners. We aim to provide for systems thinking approach to understanding cybersecurity as an interdisciplinary field of study and research. Systems thinking is discipline neutral and allows for a comprehensive approach to studying complex systems. Figure 1 summarizes this unique approach.

Figure 1: A Systems Approach to Cybersecurity Research & Policy



This leads to;



Input

Academic Readiness

NSA Educational Standards

Student Candidates

- Interest and motivation
- GPA and Degree
- Working Experience

Hands-On Experience

- Local and County CSO
  State government
  National security
- Private sector

PSU/CAE-R

MARK O. HATFIELD CENTER
FOR CYBERSECURITY

Portland State University
PHYSICAL WORLD Computers Cloud Infrastructure (Bioengines)
CYBERWORLD components
HUMAN DIMENSION Cognitive & Technical (human Security)
VIRTUAL DIMENSION Shared Digital Information environment

CAE-CD New Education Center
Academic degrees
Certificates

Job Market
Dynamic Social / Professional Context
Teachers
Goals
New Students
Students
IA Professionals
Content
Didactic Processes
Trends: Technological, Economic, Cultural, Political

Output

Professional Preparedness

National leadership

Protecting US's soft underbelly

- Information sharing lw/local govt
- Offering community assistance
- Research projects like virtual SOC
- Replicable state and local models

Cybersecurity Professionals

- Thought leaders
- Informed citizens
- Informed policy makers

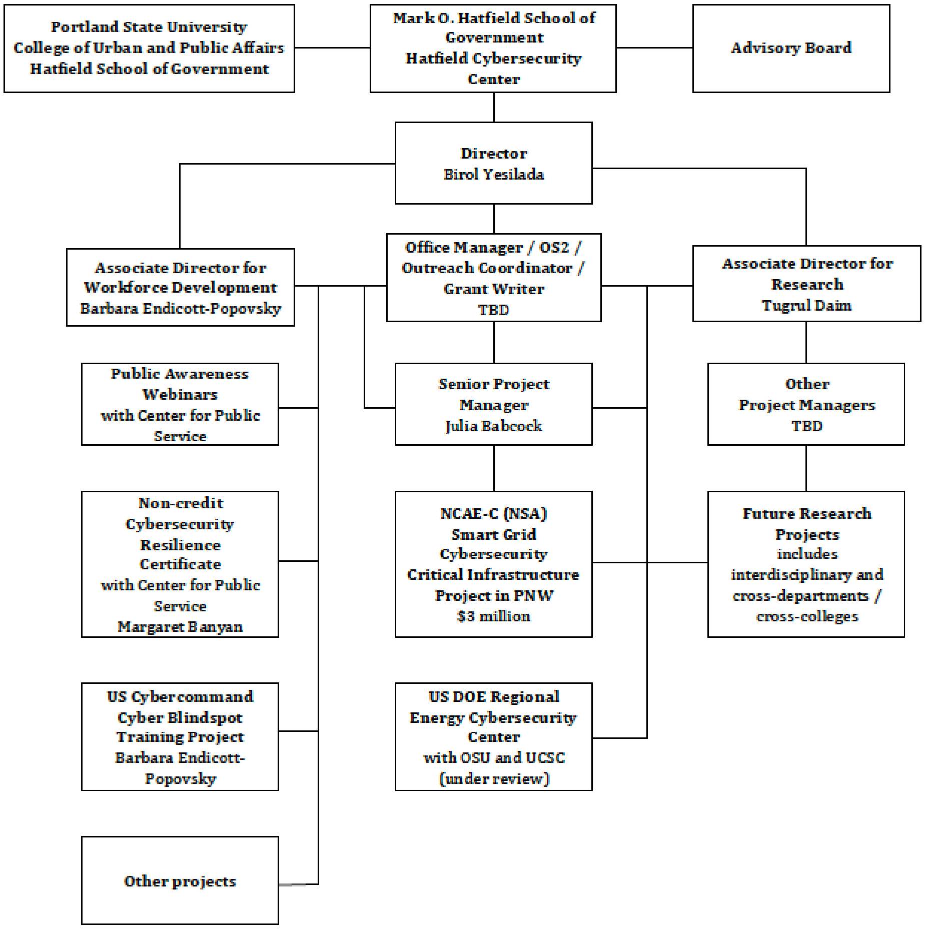
Cyber-Literate Graduates

I.	PERFORMANCE		
	Professionalism	Problem Solving Efficacy Individual Team	Continuous Learning
II.	KNOWLEDGE - SKILLS		
	Policy	Procedures	Technology
III.	ABILITIES		
	Interest & Motivation	Education (Degree, GPA, Certifications)	Experience

7. What is the proposed structure of the unit? Examples include: Where will it be housed? Will it become a separate administrative unit? Will it have its support staff? How will faculty become affiliated with the unit? Will faculty FTE be assigned to the unit? What is the likely faculty composition (% tenure-track, % fixed-term, % adjunct)? According to what rules will faculty be evaluated for P&T?

The Center will be housed in the Hatfield School of Government in the College of Urban and Public Affairs and will open to faculty affiliation from other units across PSU. See figure 2. Its membership is open to tenure-track faculty, research faculty, NTTF faculty, and research associates (who will be hired on hourly-wage agreements). The number of staff of the Center will largely depend on the scope and funding of the projects (i.e., each large project will have a project manager funded through the grant).

Figure 2: Mark O. Hatfield School Cybersecurity & Cyber Defense Policy Center


Portland State University
College of Urban and Public Affairs
Hatfield School of Government
Mark O. Hatfield School of Government
Hatfield Cybersecurity Center
Advisory Board
Director
Birol Yesilada
Associate Director for Workforce Development
Barbara Endicott-Popovsky
Office Manager / OS2 / Outreach Coordinator / Grant Writer
TBD
Associate Director for Research
Tugrul Daim
Public Awareness Webinars
with Center for Public Service
Senior Project Manager
Julia Babcock
Other Project Managers
TBD
Non-credit Cybersecurity Resilience Certificate
with Center for Public Service
Margaret Banyan
NCAE-C (NSA) Smart Grid Cybersecurity Critical Infrastructure Project in PNW
$3 million
Future Research Projects
includes interdisciplinary and cross-departments / cross-colleges
US Cybercommand Cyber Blindspot Training Project
Barbara Endicott-Popovsky
US DOE Regional Energy Cybersecurity Center
with OSU and UCSC
(under review)
Other projects

Faculty participating from units outside CUPA will choose either to have their research time paid by the grants or a portion of their positions negotiated between the Center and their home departments for a buy-out.

8. Who will have administrative oversight for the unit?

The Center will report to the Dean of CUPA (at least in the initial phase). However, its overall purpose is to serve the university in collaborative projects. In the future, as the Center's scope expands, the PSU administration might wish to have the Center based outside any single College and report directly to the Provost or VP for Research.

9. When would the unit be established? What is the period of time for the unit to operate (if it is not permanent)? Describe how the unit may evolve or expand.

The Center is to be established as soon as possible since funding is not an issue. It will be a permanent Center and a crucial member of the NCAE-C network in the country. Two projects are funded by external grants (see *White Paper*). We expect decisions on two additional contributions from the NSA as a subcontracting party to collaborative proposals. One of these projects is a regional workforce development grant with UW-Bothell and the University of Idaho at NSA. The second is another NSA proposal with the Norwich University Applied Research Institutes that would make our Center the Hub for the West Coast administration of a comprehensive training program for cybersecurity professionals in the Defense Department and US Cyber Command. As mentioned previously, our center is also identified by Oregon Legislature to be the administrative center of the future Oregon Cybersecurity Center of Excellence. If funded in the 2023 budget, this initiative would place the state-wide initiative at the Hatfield Center and coordinate between PSU, OSU, and UO. Oregon needs to have an interinstitutional collaboration to be effective in cybersecurity research and education because no single university can meet all the needs of the State. We are identified as the Hub of this initiative because of our success in receiving the NCAE-C Research designation from the NSA and DHS and the substantial grant we received for critical infrastructure research in August 2021. Please see attached Appendix for grants/projects funds.

10. What additional resources are needed for the unit? From where will these resources come? What revenue will the unit generate?
    a. Budget: Show all anticipated sources of revenue and expenditures.

Please see attached Excel sheet for the initial budget.

b. Space: Describe in detail the new space needs and where the unit would be situated.

For now, the Center can be housed on the 6th floor of CUPS in the Hatfield School. As our projects expand, we will need to consider a future site where the cybersecurity Laboratory can be financed through private sector partners and external grants.

c. Staff: Describe all anticipated workers at all levels.

Please see Figure 2 above.

d. Support Services: Describe necessary increased support services, such as additional laboratory equipment, library resources, or computers.

All necessary equipment for the Center has been ordered by grant funding. We plan to use overhead funds coming to the School of Government from these projects to purchase additional computers and other equipment.

11. List the individuals proposing the change and their departmental affiliations.

Professor Birol Yesilada, Director of the Hatfield School of Government

Professor Tugrul Daim, Department of Engineering and Technology Management (currently as research time only per grants received)

Research Professor Barbara Endicott-Popovsky, Center for Public Service and will move over to the new Center.

Signatures

Request prepared by *: *[signature]* Birol Yesilada, Ph.D, 4/21/2022

Approved by * : ____________

** Signatures are required of the immediate supervisor, and administrators at each level above that of the immediate supervisor, that approve the project prior to submission to EPC. Insert additional rows if needed.*

Reviewed by Budget Committee Chair: ____________
Date: ____________

Reviewed by Educational Policy Committee Chair: ____________
Date: ____________

Reviewed by Faculty Senate Presiding Officer: ____________
Date: ____________

Approved by Provost: ____________
Date: ____________