From: Justin Akers <jakers@sdccd.edu>
Date: Monday, October 30, 2023 at 4:11 PM
To:
Subject: RESPONSE to RE: In Response to Proposed AS Resolutions Re: Resolution Reaffirming SDCCD Commitment to Protect Undocumented Students Through Campus Sanctuary Status

Hello City Faculty,

I am sending this reply to Professor Kennemer's latest email and will make direct points that show the Cyber Defense Program is in fact collaborating with the Department of Homeland Security (DHS)--despite what Professor Kennemer claims.

1. **"**SDCC's cyber defense programs have **no partnership or affiliation or designation** with the DHS. I am fairly certain that we have shared governance and collegiality processes, that do not single out individual programs, for a topic of this nature. See my initial response about this."

Response: This was the advertisement for the recent Cyber Security Awareness Week event. As you can see, the event was co-sponsored by the "Department of Homeland Security".

Presenters included:
Experts from Amazon Web Services
David Kennemer - Esteemed Faculty, Computer Information Systems
Drew Facetti - **Renowned Manager of SD-Law Enforcement Coordination Center** – This is a DHS "Fusion center", a Department of Homeland Security project created by the DHS which include immigration enforcement agencies (see below).

---

2. **"**This was an SDCCD event held at City College that I was asked to make a short baccalaureate degree presentation in the opening. **The District's guest** was not a representative of the DHS, but in fact a cybersecurity program manager at the San Diego Law Enforcement Coordination Center."

Response: The **San Diego Law Enforcement Center** is actually a **Department of Homeland Security "Fusion Center"**. If you click the links below, it explains that the DHS created the "San Diego Law Enforcement Center":

- "The San Diego Law Enforcement Coordination Center (LECC) is San Diego's Regional Threat Assessment Center. LECC operates 24/7, providing intelligence, investigative and technical support to agencies critical to homeland security efforts in San Diego."
  https://www.dhs.gov/see-something-say-something/reporting/california/lecc
- "Fusion centers contribute to the Information Sharing Environment (ISE) through their role in receiving threat information from the federal government; analyzing that information in the context of their local environment; disseminating that information to local agencies; and gathering tips, leads, and suspicious activity reporting (SAR) from local agencies and the public. Fusion centers receive information from a variety of sources, including SAR from stakeholders within their jurisdictions, as well as federal information and intelligence. They analyze the information and develop relevant products to disseminate to their customers. These products assist homeland security partners at all levels of government to identify and address immediate and emerging threats.https://www.dhs.gov/national-network-fusion-centers-fact-sheet#:~:text=Fusion%20centers%20provide%20the%20federal,information%20to%20the%20federal%20government.
- The Department of Homeland Security, in coordination with federal interagency partners, has developed and provided a wide range of resources and services, including a guidebook, sample policies, templates, best practices, workshops, and various training sessions, to support fusion centers in strengthening their COCs and P/CRCL protections.
  https://www.dhs.gov/national-network-fusion-centers-fact-sheet
- Through these Fusion Centers, "the DHS works with the academic community - including school administrators, faculty, and students - on a range of issues. The Office of Academic Engagement (OAE) supports DHS's mission by building, improving and leveraging relationships with the academic community."
  https://www.dhs.gov/topics/academic-engagement
- The DHS is the primary federal funder of the National Network of Fusion Centers, supplying over $50 million in direct funding.
  https://www.archives.gov/files/committee-on-homeland-security-fusion-center-report-2017.pdf

---
---

3. **"Why we would ever have ICE or CBP in the classroom when they have nothing to do with cybersecurity?"**
   - Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CBP) also works through the San Diego Law Enforcement Coordination Center (LECC), and both agencies operate their own Cyber Security systems and programs and data collection processes to aid in investigations. "The U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE), Office of Homeland Security Investigations (HSI) owns and operates the Laboratory Information Management System (LIMS) as part of its Forensic Laboratory."

https://www.dhs.gov/publication/dhsicepia-046-laboratory-information-management-system

- "The U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), deploys surveillance technologies in furtherance of its criminal investigations and national security missions." https://www.dhs.gov/publication/dhsicepia-061-homeland-security-investigation-hsi-surveillance-technologies
- "The Department of Homeland Security (DHS) engages in immigration enforcement actions to prevent unlawful entry into the United States and to apprehend and repatriate noncitizens who have violated or failed to comply with U.S. immigration laws. Primary responsibility for the enforcement of immigration law within DHS rests with U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and U.S. Citizenship and Immigration Services (USCIS). CBP enforces immigration laws at and between the ports of entry, ICE is responsible for interior enforcement and for detention and removal operations, and USCIS adjudicates applications and petitions for immigration and naturalization benefits. **Each Office of Immigration Statistics (OIS) Immigration Enforcement Actions Annual Flow Report contains information obtained from CBP and ICE case records and processed by OIS to describe the number and characteristics of foreign nationals found inadmissible, apprehended, arrested, detained, returned, or removed during a given fiscal year.** https://www.dhs.gov/immigration-statistics/enforcement-actions
- For the FY 2022, the Department of Homeland Security (DHS) requested a total of 2.6 billion U.S. dollars for its entire cyber security budget, making it the largest budget among the CFO act government agencies, excluding the Department of Defense. https://www.statista.com/statistics/737504/us-fed-gov-it-cyber-security-fy-budget/#:~:text=U.S.%20federal%20government%20proposed%20cyber%20security%20spending%20FY%202022%2D2023&text=For%20the%20FY%202022%2C%20the,excluding%20the%20Department%20of%20Defense.
- Article: ICE Used Controversial Tool to Request Student Medical Records and More
- Article: ICE agents do unauthorized searches, records show

---

4. The Cyber Defense Program is not being "singled out". It has only been recently revealed that at least some aspects of the program are being developed in coordination with the DHS through the involvement of the personnel from the SD-LECC DHS Fusion Center, which allows for DHS agents to have input into the program, and most recently, to come onto our campus. These aspects of the program were not clearly stated or revealed until very recently. This opens the door for different types of involvement of immigration enforcement agents to be present and active on our campus in different capacities (job fairs, guest speakers, etc.) and creates the potential for classes or coursework that trains students on the use of immigration enforcement technologies. It will effectively end the campus sanctuary status that has been essential in creating the standards and values that define City College. We need to uphold these standards and values.
5. Professor Kennemer has stated that he agrees that it is important to protect our students and acknowledges that we are a sanctuary and social justice-focused campus that should prioritize the protection and safety of our students. **That is why we are putting forth this resolution.** It is a safeguard and assurance that the well-being of our Dreamer/DACA/undocumented students is the priority here, and that they continue to be the priority through the development and implementation of the Cyber Defense Program into the years ahead. If Professor Kennemer and others involved in the development of the Cyber Defense Program have no intention of collaborating with DHS agents, ICE, or CBP in any way, then you should *support this resolution*. That would affirm it. Otherwise, what is the argument against other than to *retain the right* to collaborate with DHS and immigration enforcement agencies? If we prioritize our students' safety and well-being, the best way we can work together is to support this resolution and move forward together as a campus that always puts our City students, their families, and their communities first.

Justin

From: David Kennemer <dkenneme@sdccd.edu>
Sent: Monday, October 30, 2023 5:30 AM
To: David Kennemer <dkenneme@sdccd.edu>
Subject: Re: In Response to Proposed AS Resolutions Re: Resolution Reaffirming SDCCD Commitment to Protect Undocumented Students Through Campus Sanctuary Status

Greetings colleagues,

It is unfortunate that I am in your inbox again so soon, but I have been encouraged to reply to the misleading points in Professor Akers' response, because I have not been afforded the opportunity to address them in person. I will do my best to refrain further replies and make this my last response.

#1 These concerns are due to the fact that when this program was first introduced, there was no mention of how curriculum was being designed in coordination with DHS standards.

Response: See my initial response to curriculum frameworks: they are **not** DHS standards. Using the two curricular frameworks for guidance has always been there, we have a curriculum review committee, council, and processes that vetted and approved this program and curricula.

#2 It was only announced for the first time that the program conformed to DHS training procedures at a Chairs meeting this semester.

Response: Professor Akers is referring to the academic discipline homeland security as the Department of Homeland Security training procedures. These are in fact two different things all together. The purpose of the Chairs' conversation was for the CCCCO defined minimum qualifications for faculty to teach in this program, in the context of hiring new faculty. As the SME, I was not present or asked for any additional information or clarification.

#3 Concerns were raised in that meeting about this very issue, but very little was stated to ensure that collaboration with DHS Agencies and agents would not be a factor that could develop.

Response: SDCC's cyber defense programs have **no partnership or affiliation or designation** with the DHS. I am fairly certain that we have shared governance and collegiality processes, that do not single out individual programs, for a topic of this nature. See my initial response about this.

#6 Recently announced public presentations relating to the program have included representatives from DHS (Cyber Security Awareness Week)

Response: This was an SDCCD event held at City College that I was asked to make a short baccalaureate degree presentation in the opening. **The District's guest** was not a representative of the DHS, but in fact a cybersecurity program manager at the San Diego Law Enforcement Coordination Center.

#10 This is not a "false narrative", it is an empirical investigation, reflection on our history, and a statement of facts and possibilities that flow from those facts. We are HERE TO SUPPORT AND SERVE OUR STUDENTS. Their safety and security should be the priority of all faculty and the institution as a whole.

Response: The fact is that the proposed resolution uses the word relationship or partnership ***five times***, in reference to our cyber defense program and the DHS, to establish something that **does not exist** and is the entire basis for this proposed resolution – so yes, it is a false narrative. Also, ask yourselves *why we would ever have ICE or CBP in the classroom when they have nothing to do with cybersecurity?* That was rhetorical, **we would not**.

Do not forget this program was vetted and approved through shared governance. Are we saying that we failed at those processes?

The reality is Professor Akers was one of a few folks who emphatically objected to this program during the shared governance process. At the time, I personally reached out to him and others offering in-depth insight and collaborative opportunities on curriculum and other ways we could address their concerns. They never engaged. **Evidence from March 2022 attached**.

Of course, we all want our students to feel safe and secure on campus. ***There is already an adopted and affirmed resolution that specifically addresses this; not by not singling out one specific program, but by applying it to the entire District.*** This proposed resolution is misleading and not who we are as a program, campus, or community.

In closing, Professor Akers said it best himself, "We are HERE TO SUPPORT AND SERVE OUR STUDENTS. Their safety and security should be the priority of **all faculty and the institution as a whole**." That, we can agree on, but this proposed resolution does not do that does it. It seeks to needlessly single out one specific program on baseless merits, discredit the shared governance process along the way.

I again encourage you to review my *entire response* and **not** support this proposed resolution.

With respect,
David

From: Justin Akers <jakers@sdccd.edu>
Date: Wednesday, October 25, 2023 at 3:01 PM
To: Justin Akers <jakers@sdccd.edu>
Subject: RE: In Response to Proposed AS Resolutions Re: Resolution Reaffirming SDCCD Commitment to Protect Undocumented Students Through Campus Sanctuary Status

In Response to David's statement:

1. These concerns are due to the fact that when this program was first introduced, there was no mention of how curriculum was being designed in coordination with DHS standards.
2. It was only announced for the first time that the program conformed to DHS training procedures at a Chairs meeting this semester.
3. Concerns were raised in that meeting about this very issue, but very little was stated to ensure that collaboration with DHS Agencies and agents would not be a factor that could develop.
4. Several people left that meeting concerned that more need to be done to protect undocumented students/dreamers.
5. There is a history of City College students and their families being victimized by DHS (ICE and Border Patrol agents) on and around our campus and serving communities.
6. Recently announced public presentations relating to the program have included representatives from DHS (Cyber Security Awareness Week)
7. We are a sanctuary campus, which means we prioritize the protection and safety of our

undocumented students

8. We are social justice campus, which prioritizes the rights, protections, and justice for our most vulnerable students.
9. If this statement "SDCC's cyber defense program has no special exclusion from this existing "sanctuary" resolution" stands as an official statement on behalf of the program, then it is appreciated and accepts as in good faith.
10. This is not a "false narrative", it is an empirical investigation, reflection on our history, and a statement of facts and possibilities that flow from those facts. We are HERE TO SUPPORT AND SERVE OUR STUDENTS. Their safety and security should be the priority of all faculty and the institution as a whole.

Justin

From: David Kennemer <dkenneme@sdccd.edu>
Sent: Wednesday, October 25, 2023 2:15 PM
To: David Kennemer <dkenneme@sdccd.edu>
Subject: In Response to Proposed AS Resolutions Re: Resolution Reaffirming SDCCD Commitment to Protect Undocumented Students Through Campus Sanctuary Status

First and foremost, greetings colleagues. I hope you are having the most awesome semester yet… and I apologize for the length of this message.

It has been brought to my attention, as the lead for our cyber defense program, a resolution presented for your consideration specifically singling out our academic program through reaffirmation of an adopted and reaffirmed resolution::The San Diego Community College District Board of Trustees stands in support of students from all backgrounds, cultures, immigration status, and religions.

At the heart of this proposed resolution is the fact that our program – as do all academic programs – uses curriculum frameworks for guidance in writing standards-based curriculum, with the common goal of developing critical knowledge, skills, and abilities (KSAs) needed to perform cybersecurity workforce roles:

The NICE Framework created by the Federal Chief Information Officers Council (FCIOC) and further led by the National Institute for Standards and Technology (NIST), under the purview of the Department of Commerce (DoC), was developed by a Core Authoring Team (CAT) that includes representatives from numerous departments and agencies in the United States federal government and "in partnership between government, academia, and the private sector working to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development."

The DCW Framework, under the purview of the Department of Defense (DoD), is a set of standardized roles and associated responsibilities that are used to classify positions within the DOD's cyber workforce, as well as a representative list of tasks and knowledge, skills and abilities (KSAs) describing what is needed to execute key functions.

The resolution continues by suggesting that because the Department of Homeland Security (DHS) is included on the NICE Framework CAT, that a relationship and potential influence exists between our program, the DHS, Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP). It is also worth noting that neither the DoC, NIST specifically, nor the DoD report to the DHS.

Let me be crystal clear, SDCC's cyber defense security programs have no relationship with the DHS, its agents, or its agencies. We are bound to all applicable District policies and procedures including the adopted and reaffirmed District "sanctuary" resolution. Further, we have declined to pursue a National Centers for Academic Excellence in Cyber Defense (NCAE-CD) education designation - despite its potential benefits for our students - because it is partly sponsored by the DHS.

Lastly, this resolution seeks to repress the academic freedom afforded to faculty as expressed through SDCCD BP 4030 Academic Freedom. Of particular concern are:

- the presumption that any individual on any campus or at the district office, whether a faculty member or not, has the right to dictate who any given faculty member may invite "to speak, present, consult, advise, or participate within the campuses, classrooms, or in the district" as found in the second to last Be it resolved on this proposed AS Resolution; and
- the presumption that any individual on any campus or at the district office, whether a faculty member or not, has the right dictate which technologies may be used or created in the classroom as expressed in the last *Be it resolved* on this proposed AS Resolution. In fact, no one can possibly know how any technology taught on any campus may be used presently or in the future.

The above language expressly inhibits the faculty or researcher's ability to investigate and discuss the issues pertinent to their academic field and/or to teach or publish findings without interference. These concepts are the mainstay of academic freedom, the same academic freedom that protects the right of a faculty member to speak freely when participating in institutional governance.

In closing, I leave you with the following tidbits and ask that you to carefully consider the implications of supporting this resolution and to encourage you to vote against it:

1. The SDCCD has already adopted and reaffirmed a "sanctuary" resolution;
2. SDCC's cyber defense program has no special exclusion from this existing "sanctuary" resolution;
3. Our program and curriculum were vetted and approved throughout the shared governance process;
4. The singling out of individual academic programs with false narratives and without consulting program subject matter experts (SMEs) is both disconcerting and absent academic collegiality.

With respect,

David

David Kennemer
Associate Professor, Computer Information Systems
San Diego City College
dkennemer@sdccd.edu

These are our official program goals and outcomes:

Goals: Upon successful program completion, our graduates will:

- Be poised to enter professional positions in a cybersecurity related occupation or continue to a graduate study in cybersecurity or a related field of interest.
- Be informed, active individuals engaged in the global community, social justice advocacy, and the highest level of professional ethics.
- Pursue lifelong learning opportunities to improve and expand their technical and professional skills.

Outcomes: Upon successful program completion, students will be able to:

- Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
- Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
- Communicate effectively in a variety of professional contexts.
- Recognize professional responsibilities and make informed judgments in computing practice, taking into account legal, ethical, diversity, equity, inclusion, and accessibility principles consistent with the mission of the institution.
- Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.
- Apply security principles and practices to maintain operations in the presence of risks and threats.