State of California Office of the Governor
Sacramento, California

READ-OUT

United States Department of Commerce
National Institute of Standards and Technology
National Initiative on Cybersecurity Education 2017 Expo & Conference in Dayton, Ohio
November 6-8, 2017

TO:	State of California CASCADE Program Partners
FROM:	Eileen Sánchez – State of California CASCADE Program Manager *California Governor's Office of Business & Economic Development (GO-Biz)* *California Governor's Office of Planning and Research (OPR)*
DATE:	November 9, 2017
RE:	Read-out of the NICE 2017 Conference in Dayton, Ohio

Summary

Cybersecurity professionals from government, industry and academia gathered last week in Dayton, OH for the annual U.S Department of Commerce, National Institute of Standards and Technology, National Initiative for Cybersecurity Education 2017 Conference and Expo (NICE 2017). Discussions focused on ways to promote and energize employers, government, businesses, educators, and the workforce to offer new opportunities to build a capable and robust cybersecurity workforce. The conference was kicked off by Rodney Petersen, Director of the NIST National Initiative for Cybersecurity Education (NICE). Keynote speakers included Tyson Meadors, Director for Cybersecurity Policy of the White House National Security Council (NSC), who joined the NSC from the Department of the Navy where he most recently served as the lead of US Fleet Cyber Command Commander's Innovation Group. Angela Messer, Executive Vice President, Booz Allen Hamilton Cyber Innovation and Talent Officer was also a keynote speaker. This year's theme was "Challenging the Status Quo: Building a Robust and Sustainable Cybersecurity Ecosystem," to help shape the way in which the nation identifies, educates, trains and builds our 21st-century cutting-edge Cybersecurity Ecosystem.

Conference tracks included:

1. Education & Training: Initiatives and innovations for identifying, recruiting, and educating the future cybersecurity workforce.
2. Collaboration: Nurturing Cybersecurity Communities in Academia, Industry, and Government
3. Professional Development: Keeping Pace with technical education, professional certifications, career development, diversity issues, retention concerns, and staff and personnel management.

The conference presented an opportunity to learn about the background, purpose and application of the National Cybersecurity Workforce Framework as well as of other Cyber security and workforce development programs, resources and available funding. To access the conference presentations, click here. For the conference agenda, click here.

For a user-friendly primer on Cyber Fundamentals, click here. For a Cyber glossary, click here.

For a comprehensive read-out of the NICE 2017 Conference, please see subsequent pages.

Read-out of the NICE 2017 Conference in Dayton, Ohio

Contents

Background

U.S. Department of Commerce, National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. NIST is headquartered in Gaithersburg, Maryland, and operates a facility in Boulder, Colorado. NIST's activities are organized into laboratory programs and extramural programs.

NIST Laboratories include:

- Center for Nanoscale Science and Technology (CNST)
- Communications Technology Laboratory (CTL)
- Engineering Laboratory (EL)
- Information Technology Laboratory (ITL)
- NIST Center for Neutron Research (NCNR)
- Material Measurement Laboratory (MML)
- Physical Measurement Laboratory (PML)

Extramural programs include:

- Hollings Manufacturing Extension Partnership (MEP), a nationwide network of centers to assist small and mid-sized manufacturers to create and retain jobs, improve efficiencies, and minimize waste through process improvements and to increase market penetration with innovation and growth strategies.
- Technology Innovation Program (TIP), a grant program where NIST and industry partners cost share the early-stage development of innovative but high-risk technologies.

National Initiative for Cybersecurity Education (NICE)

The National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce leads the National Initiative for Cybersecurity Education (NICE). It is an initiative to foster partnerships between government, academia, and the private sector focused on national cybersecurity education, training, and workforce development to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure. The NICE Program Office operates under the Applied Cybersecurity Division, located in the Information Technology Laboratory at NIST, positioning the program to support the country's ability to address current and future cybersecurity challenges through standards and best practices.

Comprehensive National Cybersecurity Initiative of 2008 (CNCI)

NICE was launched in April 2010 by the Obama Administration to represent the continual evolution of Comprehensive National Cybersecurity Initiative (CNCI) of 2008, which was established by President George W. Bush in *National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)* in January 2008. The CNCI outlined U.S. cybersecurity goals and spanned multiple agencies including the Department of Homeland Security, the Office of Management and Budget, and the National Security Agency. Initial signing of the initiative and hearings about the initiative during 2008 were kept classified. The goals of the initiative included: establishing a front line of defense against network intrusion; defending the U.S. against the full spectrum of threats through counterintelligence; and strengthening the future cybersecurity environment through education, coordination and research. In May 2009, the Obama Administration announced that it agreed with the recommendations of the resulting U.S. Cyberspace Policy Review that identified enhanced information

sharing as key component of effective cybersecurity, and the Administration launched the following CNCI initiatives to assure a trusted and resilient information and communications:

1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections (TIC).
2. Deploy an intrusion detection system of sensors across the Federal enterprise (EINSTEIN 2).
3. Pursue deployment of intrusion prevention systems across the Federal enterprise (EINSTEIN 3).
4. Coordinate and redirect research and development (R&D) efforts.
5. Connect current cyber ops centers to enhance situational awareness.
6. Develop and implement a government-wide cyber counterintelligence (CI) plan.
7. Increase the security of our classified networks.
8. Expand cyber education and develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees.
9. Define and develop enduring "leap-ahead" technology, strategies, and programs.
10. Define and develop enduring deterrence strategies and programs.
11. Develop a multi-pronged approach for global supply chain risk management.
12. Define the Federal role for extending cybersecurity into critical infrastructure domains.

For descriptions of each initiative, click here.

In March 2010 the Obama administration declassified limited material regarding the project, and announced that the CNCI scope had expanded from a federal focus to a larger national focus. With education as one of the key CNCI initiatives (number 8), starting in April 2010, the National Initiative for Cyber Security Education (NICE) represented the continual evolution of the CNCI, with NIST assuming the overall coordination role.

For the NICE announcement, click here.

Cybersecurity Act of 2015

The Cybersecurity Information Sharing Act was introduced on July 10, 2014 during the 113th Congress, and was able to pass the Senate Intelligence Committee by a vote of 12-3.The bill did not reach a full senate vote before the end of the congressional session. The bill was reintroduced for the 114th Congress on March 12, 2015, and the bill passed the Senate Intelligence Committee by a vote of 14-1. On December 18, **2015**, President Obama signed into law the Cybersecurity Act of 2015.

In summary, the Act established a mechanism for cybersecurity information sharing among private sector and federal government entities. The main provisions of the bill intended to make it easier for companies to share personal information with the government, especially in cases of cyber security threats. Without requiring such information sharing, the bill creates a system for federal agencies to receive threat information from private companies. With respect to privacy, the bill included provisions for preventing the act of sharing data known to be both personally identifiable and irrelevant to cyber security. Any personal information which does not get removed during the sharing procedure could be used in a variety of ways. These shared cyber threat indicators can be used to prosecute cyber crimes, but may also be used as evidence for crimes involving physical force.

Click here for a full summary.

Cybersecurity National Action Plan (CNAP)

In February 2016, President Obama directed the Administration to implement a Cybersecurity National Action Plan (CNAP) to take short-term actions and put in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security. Fundamentally, CNAP was intended to try to bring alive some of the things mentioned in the Cybersecurity Act of 2015, which the U.S. Congress had passed in December 2015. It primarily encourages the private sector to share security events with one another and the federal government. CNAP introduced six key changes:

1. Creating a blue-ribbon Commission on Enhancing National Cybersecurity, which serves to provide a series of recommendations and actions that strengthen cybersecurity in both the private sector and federal agencies.
2. Establishing a new $3.1-billion Information Technology Modernization Fund, to be included in the following year federal budget for the modernization of various government IT systems.
3. Create a Federal Chief Information Security Officer, the first such position in the federal bureaucracy (although in the past federal CIOs existed in various agencies). The top salary offered is $185,000 and the position will be based in the OMB office. Candidates were recruited in February of 2016.
4. Launching a National Cybersecurity Awareness Campaign, and include (among other things) promoting authentication tools and techniques for private citizens to improve their account-access security. Part of this aimed to incorporate efforts to stop using social security numbers as an identifier of citizens by select federal agencies.
5. Adding $19 billion (more than a one-third increase) to next year's federal budget for a variety of federal programs related to cybersecurity.
6. Aim to double the number of federal civilian cyber-defense teams in the Department of Homeland Security to a total of 48. This also meant trying to recruit the best cybersecurity heads from across the federal government and private sector for these teams.

Office of the Director of National Intelligence (ODNI)

The **Director of National Intelligence** (**DNI**) is the United States government cabinet-level official – subject to the authority, direction, and control of the President – required by the Intelligence Reform and Terrorism Prevention Act of 2004 to:

- Serve as head of the seventeen-member United States Intelligence Community,
- Direct and oversee the National Intelligence Program; and
- Serve as an advisor, upon invitation, to the President and his executive offices of the National Security Council, and the Homeland Security Council about intelligence matters related to national security.

On July 30, 2008, President George W. Bush issued Executive Order 13470, amending Executive Order 12333 to strengthen the DNI's role. Further, by Presidential Policy Directive 19 signed by Barack Obama in October 2012, the DNI was given overall responsibility for Intelligence Community whistleblowing and source protection. Dan Coats is the current director.

Working together with the Principal Deputy DNI and with the assistance of Mission Managers and Deputy Directors, the Office of the DNI's goal is to effectively integrate foreign, military and domestic intelligence in defense of the homeland and of United States interests abroad.

Cyber Threat Framework

The Cyber Threat Framework was developed by ODNI to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. The Cyber Threat Framework is applicable to anyone who works cyber-related activities, its

principle benefit being that it provides a common language for describing and communicating information about cyber threat activity. The framework and its associated lexicon provide a means for consistently describing cyber threat activity in a manner that enables efficient information sharing and cyber threat analysis, that is useful to both senior policy/decision makers and detail oriented cyber technicians alike.

Fundamentals of Cyber (E-Learning Modules)

From a "Cyber" beginner perspective, I thought that DNI provided the best basic information. It is very user friendly.

Cyber Glossary

The ODNI Cyber glossary is also a great primer.
https://www.dni.gov/e-Learning_CyberExplore/pdf/Cyber_Explore_Glossary.pdf

DNI Centers

- Cyber Threat Intelligence Integration Center
- National Counterproliferation Center
- National Counterintelligence and Security Center
- National Counterterrorism Center

United States Intelligence Community (IC)

The U.S. Intelligence Community is a coalition of 17 agencies and organizations, including the ODNI. The IC agencies fall within the Executive Branch, and work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities. The IC was established by Executive Order 12333, signed on December 4, 1981, by U.S. President Ronald Reagan.

Members

	Federal Department	Parent Agency	Agency
1	Defense	United States Air Force	Twenty-Fifth Air Force
2	Defense	United States Army	Intelligence and Security Command
3	Defense	*none*	Defense Intelligence Agency
4	Defense	United States Marine Corps	Marine Corps Intelligence Activity
5	Defense	*none*	National Geospatial-Intelligence Agency
6	Defense	*none*	National Reconnaissance Office
7	Defense	*none*	National Security Agency/Central Security Service
8	Defense	United States Navy	Office of Naval Intelligence
9	Energy	*none*	Office of Intelligence and Counterintelligence
10	Homeland Security	United States Coast Guard	Coast Guard Intelligence
11	Homeland Security	*none*	Office of Intelligence and Analysis
12	Independent agency	*none*	Central Intelligence Agency
13	Justice	Drug Enforcement Administration	Office of National Security Intelligence
14	Justice	Federal Bureau of Investigation	Intelligence Branch
15	State	*none*	Bureau of Intelligence and Research
16	Treasury	*none*	Office of Terrorism and Financial Intelligence

Executive Order 12333 charged the IC with six primary objectives:

1. Collection of information needed by the President, the National Security Council, the Secretary of State, the Secretary of Defense, and other executive branch officials for the performance of their duties and responsibilities;
2. Production and dissemination of intelligence;
3. Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the U.S., international terrorist and/or narcotics activities, and other hostile activities directed against the U.S. by foreign powers, organizations, persons and their agents;
4. Special activities (defined as activities conducted in support of U.S. foreign policy objectives abroad which are planned and executed so that the "role of the United States Government is not apparent or acknowledged publicly", and functions in support of such activities, but which are not intended to influence United States political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions);
5. Administrative and support activities within the United States and abroad necessary for the performance of authorized activities and
6. Such other intelligence activities as the President may direct from time to time.

The White House National Security Council (NSC)

The White House National Security Council (NSC) is the principal forum used by the President of the United States for consideration of national security and foreign policy matters with senior national security advisors and Cabinet officials and is part of the executive office of the president of the United States. The Council also serves as the president's principal arm for coordinating these policies among various government agencies. The National Security Council was created in 1947 by the National Security Act. The predecessor to the National Security Council was the National Intelligence Authority (NIA), which was established by President Truman's Executive Letter of January 22, 1946 to oversee the Central Intelligence Group, the CIA's predecessor. The NIA was composed of the Secretary of State, Secretary of War, Secretary of the Navy, and the Chief of Staff to the Commander in Chief. It was created in an attempt to ensure coordination and concurrence among the Army, Marine Corps, Navy, Air Force and other instruments of national security policy such as the Central Intelligence Agency (CIA), also created in the National Security Act. In 2004, the position of Director of National Intelligence (DNI) was created, taking over the responsibilities previously held by the head of CIA, the Director of Central Intelligence, as a cabinet-level position to oversee and coordinate activities of the Intelligence Community. On May 26, 2009, President Obama merged the White House staff supporting the Homeland Security Council (HSC) and the National Security Council into one National Security Staff (NSS). The HSC and NSC each continue to exist by statute as bodies supporting the President. The name of the staff organization was changed back to National Security Council Staff in 2014. On January 29, 2017, President Donald Trump restructured the Principals Committee (a subset of the full National Security Council), while at the same time altering the attendance of the Chairman of the Joint Chiefs of Staff and Director of National Intelligence.

Take-Aways and Federal Cybersecurity Education Resources

National Initiative for Cybersecurity Education (NICE)

National Cybersecurity Workforce Framework

- The National Cybersecurity Workforce Framework serves as a fundamental reference to support a workforce capable of meeting an organization's cybersecurity needs. It provides organizations with a common, consistent lexicon that categorizes and describes cybersecurity work by Category, Specialty

Area, and Work Role. It is a resource from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.

- NIST released the most recent version of the Framework on August 7, 2017 as NIST Special Publication 800-181, the NICE Cybersecurity Workforce Framework. NIST posted the first NICE Framework for public comment in September 2012 and it published as final in April 2013 as the National Cybersecurity Workforce Framework version 1.0. The National Cybersecurity Workforce Framework version 2.0 posted in April 2014.
- During the NICE 2017 conference, government and academic colleagues from Australia, Canada and Singapore were present to learn of the new updates and application of the framework.
- The NICE Framework is a living document that is updated periodically based on change requests to the NICE Program Office. NICE will consider recommendations (change requests) for expansion, update/correction, withdrawal, or integration of NICE Framework components using the process described below. NIST is looking to us for comments from Subject Matter Experts to shape a better national framework. For the "change request", click here.
- DoD CIO Key Point of Contact, Stephanie Keith, Chief of Cyber Workforce Strategy & Policy Division has been a lead contributor to the Framework. For a DoD presentation on Cyber Workforce & Skill Communities, click here.
- The right panel of the NICE website includes updated resources such as a Reference Spreadsheet for the NICE Framework, NIST SP 800-181 (September 8, 2017)
- NIST will add cybersecurity competencies into a new draft version of NIST SP 800-16 , a Role-Based Model for Federal Information Technology / Cybersecurity Training. The new draft SP 800-16 will include most of the competencies shown in this Competencies to NICE framework mapping spreadsheet.
- A key challenge has been on the application of the framework, and figuring out better ways for employers to utilize it. There seems to be a lack of connectedness between the academic aspect of the framework and the reality of what businesses and employers need (even re NIST Framework for Critical Infrastructure). The closest "lync" at this point is NIST 800-73 Rev 1.

Work Role Capability Indicators

- NIST and DHS shared that everyone can agree that the NICE Framework defines the spectrum of cybersecurity work as well as tasks and knowledge, skills, and abilities (KSAs) for over 50 common Work Roles, and that Work Roles have made the NICE Framework easier to associate to specific positions. However, they do not provide organizations with guidance on how to determine if a professional can perform a Work Role.
- During the conference, NIST and DHS released a new draft report NIST Interagency Report (NISTIR) 8193 NICE Framework Work Role Capability Indicators, to help address this challenge. The report is co-authored by representatives from the U.S. Department of Homeland Security, National Institute of Standards and Technology, and Booz Allen Hamilton Inc., to help determine what qualities or accomplishments indicate that someone is suitable to perform a particular job or activity. These qualities are defined in this report as "capability indicators."
- Capability indicators are recommended education, certification, training, experiential learning, and continuous learning that could signal an increased ability to perform a given Work Role. Though capability indicators are not formal qualification requirements, they provide a menu of characteristics recommended by subject matter experts (SMEs) that should be customized by each organization based on need and incorporated into hiring and employee development efforts (e.g., recruiting, building career paths). Overarching findings pertaining to capability indicators across Work Roles and proficiency levels are also provided in this report.

- **NIST and DHS welcome comments from California. Comments are due by December 8, 2017 via email to cybersecurityworkforce@hq.dhs.gov. This is great opportunity to underscore the need for cybersecurity work roles to exist beyond just info tech.**
- The urgency to establish the capability indicators starts with the initial findings from subject matter experts. Posting it for public comment seeks to broaden the data and advance the conversation about how organizations can develop their qualifications for the work roles performing cybersecurity work.

Working Group (NICEWG)

- NICE holds monthly working group meetings, National Initiative for Cybersecurity Education Working Group (NICEWG), to provide a mechanism in which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development. They are looking for participants from California.
- The working groups are comprised of five sub-working groups. Each subgroup meets independent of the NICEWG and reports out at the NICEWG Meetings. The subgroups are: K-12, Collegiate, Competitions, Training and Certifications and Workforce Management. Click here to read the full NICE Working Group Charter.
- For more information on the working group meetings, click here.
- Ken Slaght from the California Governor's Military Council, San Diego Cyber Center of Excellence and former head of Spawar co-chairs the Training and Certifications sub-working group. The chair is Linda Montgomery, President of Cyber World Institute: Email: lmontgomery@tlclasvegas.com; Direct line: (702) 933-4700; Cell phone: (702) 528-0945.

National Cybersecurity Career Awareness Week and Cybersecurity Challenge

- The National Cybersecurity Career Awareness Week is a celebration to focus local, regional, and national interest to inspire, educate and engage children through adults to pursue careers in cybersecurity. Cybersecurity Career Awareness Week takes place during November's National Career Development Month, and each day of the week-long celebration provides for learning about the contributions, innovations and opportunities that can be found by exploring cybersecurity as a field of study or career choice.
- During the week, learners of all ages, educators, parents, employers and the community participate in a national recognition of how cybersecurity plays a vital role in the lives of Americans and how building a national cybersecurity workforce enhances America's national security and promotes economic prosperity.
- Activities and initiatives during the week are intended to build awareness of the broad array of career opportunities available to students and adults.
- The National Cybersecurity Career Awareness Week Cybersecurity Challenge is a nation-wide challenge for educators, students, career counselors, and others that will ignite interest in cybersecurity careers by enabling participants to test drive cybersecurity careers with a free online cybersecurity career exploration platform called the NSA Day of Cyber (details under NSA section).
- The National Cybersecurity Career Awareness Week Cybersecurity Challenge will launch at the first annual National Cybersecurity Career Awareness Week Kick-off event and run until December 5th, 2017 where the top 5 schools will be announced at the National K-12 Cybersecurity Education Conference in Nashville, Tennessee.

NICE Apprenticeships

Marian Merritt, the Lead for Industry Engagement at the National initiative for Cybersecurity Education (NICE), led a pre-conference seminar on the importance of apprenticeships for business from the

perspective of the federal government. Marian provided a view into the importance of moving away from just internships to apprenticeships, or even "residencies", in order to more effectively train and educate workforce. Internships would be considered more short-term periods of temporary work experience, typically lasting for a few weeks or months. An apprenticeship would be considered a more formal employment program that trains individuals to do a specific job. Unlike internships, apprenticeships employ people who already know which career path they wish to follow. In an apprenticeship, the individual typically signs a contract with their employer and the individual learns specific skills during their apprenticeship. This usually includes a mix of on-the-job training and work experience, and formal, classroom-based learning. Programs can last from one to six years, and at the end of your apprenticeship, you'll have a formal qualification and the skills needed to work in your chosen field.

The concept of cybersecurity residencies is still novel. A cybersecurity residency would be considered field experience that allows a student to observe and document how cyber security working professionals perform their job responsibilities. Students would also participate to a limited extent in performing tasks under supervision by cybersecurity program professors and on-site staff. Concurrently, students enroll in a course, which outlines the expectations and requirements of the residency. The expectations associated with the residency would vary according to the career. For example, a practicum in teaching may require assisting the teacher with implementing small group instruction, whereas a practicum in nursing may entail recording vital signs for one or two patients under supervision. General characteristics of cyber security residencies could include: (1) Shadowing one or more assigned cyber security employees who will guide the on-site experience. (2) Observing and correlating practices in the field with theories and methods previously studied; and (3) Recording data or assisting with tasks as directed by on-site cyber security personnel. Completing cyber security residency course assignments. Participation at the practicum site is typically two or three times per week for a few hours per session. No remuneration is expected for a residency, but it does qualify for academic credit.

For Apprenticeship Forward information, click here. NICE also hosts a webinars on Building Your Cybersecurity Team with Apprenticeships. Click here to view the recording. The PowerPoint slides used during the webinar can be downloaded here. To access the NICE Webinar Series, click here. Other resources:

- National Apprenticeship Week
- ISC(2) 2015 Global Information Security Workforce Study
- State of Cybersecurity Implications for 2016

NICE Challenge

- The NICE Challenge Project is a National Institute of Standards and Technology (NIST) and National Security Agency (NSA) grant project managed and staffed by the 501(c)(3) non-profit University Enterprises Corporation (UEC) in partnership with California State University, San Bernardino.
- The NICE Challenge Project aims to develop virtual challenges and environments to test students and professionals alike (in academic settings) on their ability to perform NICE Cybersecurity Workforce Framework tasks and exhibit their knowledge, skills, and abilities.

Cyber Ranges

- Cyber ranges are interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment.
- During the NICE conference, it was made visible that States like Massachusetts, Ohio, Michigan and Colorado are leading in this space.
- Cal Poly San Luis Obispo's facilities were also often mentioned. For additional information on the facilities, see page 28.

- Cyber Ranges are intended to provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing. A cyber range may include actual hardware and software or may be a combination of actual and virtual components.
- Ranges may be interoperable with other cyber range environments. The Internet level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email as needed by the customer.
- For more NIST information on Cyber Ranges, click here.
- For some examples of Cyber Ranges, click: CISCO, IBM, State of Michigan, and U.S. Army.

Cybersecure Communities

The National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) will jointly sponsor the 2018 Global City Teams Challenge (GCTC), which will focus on designed-in cybersecurity for "smart city" systems that are more secure, reliable, resilient and protective of privacy. Contact: Chad Boutin; boutin@nist.gov; (301) 975-4261. This is potentially a good opportunities for cyber leader cities like San Diego to participate in this program.

NICE 1-Pagers

- Cybersecurity Competitions
- Workforce Demand
- Cyber Ranges
- NICE Cybersecurity Workforce Framework
- Cybersecurity Apprenticeships
- Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development
- National Centers of Academic Excellence in Cybersecurity
- Advanced Technological Education Program
- Cybercorps: Scholarships for Service (SFS)

U.S. National Science Foundation

The National Science Foundation grants hundreds of cybersecurity research awards each year. Based on active research in this area, they have created a list of hot topics in the field, with working definitions and examples of each. Click here to view. Here are some key workforce related funding areas:

Cybersecurity Education & Jobs

Training to ensure that ethical cybersecurity experts are available for service in government and industry. NSF funds basic research in cybersecurity together with research on learning, as well as a number of cybersecurity education programs, to address this challenge.

Similarly, protecting cyberspace requires a cybersecurity workforce that can rapidly detect and respond to threats and create ways to thwart attacks by design before they occur. More than ten thousand cybersecurity workers are needed by the government and many more are required by industry.

In a NSF-funded simulation planned for students in the cybersecurity program at California State University, San Bernardino (CSUSB) via the CyberCorps®: Scholarships for Service (SFS) program, undergraduate and graduate students are taking interdisciplinary approach to cybersecurity. "We provide an environment where business students can work with engineers on drones, and students from political science can work on predictive modeling," said Principal Investigator (PI) Tony Coulson, Professor at

CSUSB College of Business and Public Administration, Information & Decision Sciences; Email:tcoulson@csusb.edu; Phone:(909) 537-5768.

CyberCorps(R) Scholarship for Service (SFS)

The CyberCorps(R): Scholarship for Service (SFS) program is seeking proposals that address cybersecurity education and workforce development. The *Scholarship Track* provides funding to award scholarships to students in cybersecurity. All scholarship recipients must work after graduation for a Federal, State, Local, or Tribal Government organization in a position related to cybersecurity for a period equal to the length of the scholarship.

A proposing institution must provide clearly documented evidence of a strong existing academic program in cybersecurity. Such evidence can include: designation by the National Security Agency and the Department of Homeland Security as a Center of Academic Excellence in Information Assurance Education/Cyber Defense (CAE IA/CD), in Cyber Operations or in Research (CAE-R); a specialized designation by a nationally recognized organization (for example, in forensics); or equivalent evidence documenting a strong program in cybersecurity.

Full Proposal Window: November 17, 2017 - December 5, 2017
https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991

U.S. Department of Homeland Security (DHS)

DHS coordinates with sector specific agencies, other federal agencies, and private sector partners to share information on and analysis of cyber threats and vulnerabilities and to understand more fully the interdependency of infrastructure systems nationwide. This collective approach to prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents prioritizes understanding and meeting the needs of our partners, and is consistent with the growing recognition among corporate leaders that cyber and physical security are interdependent and must be core aspects of their risk management strategies.

National Initiative for Cybersecurity Careers and Studies (NICCS)

- The National Initiative for Cybersecurity Careers and Studies (NICCS) is an online resource for citizens to find the cybersecurity education and training they need to advance their careers and close the skill gaps in the cybersecurity workforce. NICCS is managed the U.S. Department of Homeland Security's (DHS) Office of Cybersecurity and Communications (CS&C), Cybersecurity Education and Awareness Branch (CE&A).
- The NICCS Education and Training Catalog is a central location where people across the nation can search over 3,000 cybersecurity-related courses by visiting: https://niccs.us-cert.gov/training/search
- There are approximately 102 providers in California listed on this catalogue.
- The courses in the training catalog are cybersecurity focused and delivered by accredited universities, National Centers of Academic Excellence, federal agencies, and other training providers. Each course is mapped to the NIST National Cybersecurity Workforce Framework, the foundation of the National Initiative for Cybersecurity Education (NICE) effort to standardize the cybersecurity field.
- Over 30,000 people visit NICCS each month, and prospective students run over 6,000 unique searches in the Education and Training Catalog, making NICCS the place to promote cybersecurity related training courses. For organizations or academic institutions interested in listing courses, they may just apply to become a provider by filling out the Vendor Vetting Form.
- DHS CE&A promotes cybersecurity awareness, training, and education and career structure, with the added goal of broadening the Nation's volume of cybersecurity workforce professionals.

- Through the NICCS online resource, there is a tool to write position descriptions around the NICE framework, so that there is a path for people. Nonetheless, during the conference, it was discussed that often the challenge is not creating new job roles, it is convincing HR.

National Cybersecurity and Communications Integration Center (NCCIC)

- DHS's National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.
- The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost. The NCCIC is comprised of four branches: (1) NCCIC Operations and Integration (NO&I); (2) United States Computer Emergency Readiness Team (US-CERT); (3) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT); and (4) National Coordinating Center for Communications (NCC).

United States Computer Emergency Readiness Team (US-CERT)

- The NCCIC four products in the US-CERT National Cyber Awareness System offer a variety of information for users with varied technical expertise. Those with more technical interest can read the Alerts, Current Activity, or Bulletins. Users looking for more general-interest pieces can read the Tips.
- The US-CERT Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to US-CERT. This system assists analysts in providing timely handling of security incidents as well as the ability to conduct improved analysis. If a business or individual would like to report a computer security incident, the need to complete the following form: https://www.us-cert.gov/forms/report.
- The Law Enforcement Cyber Incident Reporting resource provides information for state, local, tribal, and territorial (SLTT) law enforcement on when, what and how to report a cyber incident to a federal entity. The document also provides information on federally sponsored training opportunities and other useful resources available to SLTT law enforcement.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

- The NCCIC Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

National Coordinating Center for Communications (NCC)

The NCCIC National Coordinating Center for Communications (NCC) continuously monitors national and international incidents and events that may impact emergency communications. Incidents include not only acts of terrorism, but also natural events such as tornadoes, floods, hurricanes and earthquakes. In cases of emergency, NCC Watch leads emergency communications response and recovery efforts under Emergency Support Function #2 of the National Response Framework.

National Infrastructure Coordinating Center (NICC)

The National Infrastructure Coordinating Center (NICC), which is part of the DHS National Operations Center, is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government. When an incident or event affecting critical infrastructure occurs and requires coordination between DHS and the owners and operators of our Nation's critical infrastructure, the NICC serves as that information sharing hub to support the security and resilience of these vital assets.

The NICC and the NCCIC share cyber and physical security information to enhance the efficiency and effectiveness of the U.S. government's work to secure critical infrastructure and make it more resilient.

Critical Infrastructure Sectors

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

1. Chemical Sector
2. Commercial Facilities Sector
3. Communications Sector
4. Critical Manufacturing Sector
5. Dams Sector
6. Defense Industrial Base Sector
7. Emergency Services Sector
8. Energy Sector
9. Financial Services Sector
10. Food and Agriculture Sector
11. Government Facilities Sector
12. Healthcare and Public Health Sector
13. Information Technology Sector
14. Nuclear Reactors, Materials, and Waste Sector
15. Transportation Systems Sector
16. Water and Wastewater Systems Sector

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

Critical Infrastructure Cyber Community Voluntary Program (C^3VP)

- DHS has partnered with the critical infrastructure community to establish a voluntary program to encourage use of the Framework for Improving Critical Infrastructure Cybersecurity to strengthen critical infrastructure cybersecurity.
- The Critical Infrastructure Cyber Community C^3 (pronounced "C Cubed") Voluntary Program is the coordination point within the federal government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The C^3 Voluntary Program aims to support industry in increasing its cyber resilience; increase awareness and use of the Framework for Improving Critical Infrastructure Cybersecurity; and encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management.

U.S Department of Defense, National Security Agency (NSA)

- The National Security Agency (NSA) is a national-level intelligence agency of the United States Department of Defense, under the authority of the Director of National Intelligence. The NSA is responsible for global monitoring, collection, and processing of information and data for foreign intelligence and counterintelligence purposes, specializing in a discipline known as signals intelligence (SIGINT).
- The NSA is also tasked with the protection of U.S. communications networks and information systems. The NSA relies on a variety of measures to accomplish its mission, the majority of which are covert. Originating as a unit to decipher coded communications in World War II, it was officially formed as the NSA by President Harry S. Truman in 1952. Since then, it has become one of the largest U.S. intelligence organizations in terms of personnel and budget.
- There are two types of designations for NSA Centers of Academic Excellence (CAEs) in Cyber. One is not to be confused with the other. (1): National Centers of Academic Excellence in Cyber Defense and (2) National Centers of Academic Excellence in Cyber Operations.

National Centers of Academic Excellence in Cyber Defense (CAE-CD) program

- NSA and DHS jointly sponsor the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program. The goal is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise for the Nation.
- Over 200 top colleges and universities across 44 states, the District of Columbia, and Puerto Rico are designated CAEs for cyber-related degree programs. Specific 2 and 4-year colleges and universities are designated based on their robust degree programs and close alignment to specific cybersecurity-related knowledge units (KUs), validated by top subject matter experts in the field.
- By attending a CAE institution, students have the opportunity to learn by doing and to contribute their efforts to the protection of our nation.
- For more info on CAEs in Cyber Defense, click here. For CAE-CD program guidance, requirements and resources click here. For a current list of NSA/DHS CAE institutions, click here.

California National Centers of Academic Excellence in Cyber Defense

Institution	Designation	Designated	Expiration
California State Polytechnic University, Pomona	CAE-CDE 4Y	2014	2021
California State University, Sacramento	CAE-CDE 4Y	2017	2022
California State University, San Bernardino	CAE-CDE 4Y	2014	2021
Coastline Community College	CAE-CDE 2Y	2014	2019
National University	CAE-CDE 4Y	2014	2020
Naval Postgraduate School	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
San Jose State University	CAE-CDE 4Y	2014	2019
University of California, Davis	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021

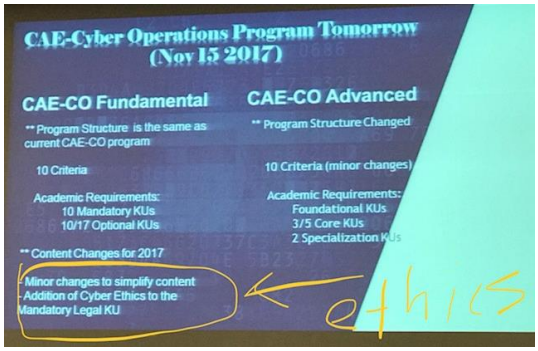
University of California, Irvine	CAE-R	2014	2019

Designations:
CAE/IAE 4Y- National Centers of Academic Excellence in Information Assurance Education
CAE-CDE 4Y- National Centers of Academic Excellence in Cyber Defense Education
CAE/IAE 2Y - National Centers of Academic Excellence in Information Assurance 2-Year Education
CAE-CDE 2Y - National Centers of Academic Excellence in Cyber Defense 2-Year Education
CAE-IA-R - National Centers of Academic Excellence in Information Assurance Research
CAE-R - National Centers of Academic Excellence in Cyber Defense Research

National Centers of Academic Excellence in Cyber Operations (CAE in Cyber Ops)

- The National Security Agency's (NSA) National Centers of Academic Excellence (CAE) in Cyber Operations Program is intended to be a deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science (CS), computer engineering (CE), and/or electrical engineering (EE) disciplines, with extensive opportunities for hands-on applications via labs/exercises.
- Only 19 academic institutions (listed below) are currently designated as NSA Centers of Academic Excellence in Cyber Operations, one is from California:
    1. Air Force Institute of Technology (Ohio)
    2. Auburn University (Alabama)
    3. Carnegie Mellon University (Pennsylvania)
    4. Dakota State University (South Dakota)
    5. Mississippi State University (Mississippi)
    6. **Naval Postgraduate School (California)**
    7. Northeastern University (Massachusetts)
    8. New York University Tandon School of Engineering (New York)
    9. Texas A&M University (Texas)
    10. Towson University (Maryland)
    11. United States Air Force Academy (Colorado)
    12. United States Military Academy at West Point (New York)
    13. University of Cincinnati (Ohio)
    14. University of Nebraska Omaha (Nebraska)
    15. University of New Orleans (Louisiana)
    16. University of Texas at Dallas (Texas)
    17. University of Texas at El Paso (Texas)
    18. University of Tulsa (Oklahoma)
    19. Virginia Polytechnic Institute and State University (Virginia)
- For a detailed list of the current CAEs in Cyber Ops with information on the academic years for the designation, and the level of study that has met the criteria, click here.
- When we asked “why not more from California”, the speakers clarified that this is a very technical program, and they tend to see more “Cyber Leadership” talent from California vs. “Cyber Operations” talent. The NSA CAE Cyber Ops designation is also highly technical.

- Click here for Criteria for Measurement, Academic Requirements for Designation and the Program Application.
- The CAE-Cyber Operations program complements the existing Centers of Academic Excellence (CAE) in Cyber Defense (CAE-CD) programs, providing a particular emphasis on technologies and techniques related to specialized cyber operations (e.g., collection, exploitation, and response).
- I was pleased to see that the new content requirements will include Cyber Ethics.



Cyber Incident Response Assistance (CIRA)

The Cyber Incident Response Assistance (CIRA) accreditation was designed to meet the growing needs of the U.S. Government, supplementing the incident response and intrusion detection services that NSA/IAD provides to the DOD, IC, and other organizations as authorized and directed. The core objective of CIRA accreditation is to identify companies qualified to provide rapid, on-site support to National Security Systems (NSS) owners and operators in incident response and intrusion detection. Broadly speaking, assessment of capabilities is based on the ability to:

- Consistently deliver services using repeatable processes and procedures.
- Assign highly skilled and qualified staff, who are eligible to hold U.S. Government Security clearances, to follow outlined processes and procedures to deliver services.
- Maintain and improve the quality of delivered services through training initiatives, improvement of analytical capabilities, and use of lessons learned from previous deployments or engagements to refine processes.

CIRA accreditation is awarded to qualified CIRA providers who are capable of providing comprehensive CIRA services to operators of classified and unclassified National Security Systems (NSS).

Vulnerability Assessment Service (VAS)

The Vulnerability Assessment (VA) accreditation was designed to meet the growing needs of the U.S. government, supplementing the vulnerability assessment/security scanning services that NSA/IAD provides to the Department of Defense (DOD), Intelligence Community (IC), and other organizations as authorized and directed. The core objective of VA accreditation is to recognize service providers that are available to supplement, not to replace, the internal capabilities of the owners, operators, and certifiers of classified and unclassified National Security Systems and qualified to provide rapid, on-site support services to National Security Systems (NSS) owners and operators and Government Community Customers (GCC) in vulnerability assessment. Broadly speaking, assessment of capabilities is based on the provider's ability to:

- Consistently deliver VA services using thoroughly documented, repeatable processes, and procedures.
- Assign highly skilled and qualified staff who are eligible to hold U.S. Government security clearances to follow the aforementioned processes and procedures to deliver VA services.
- Maintain and improve the quality of delivered services through training initiatives, improvement of analytical capabilities, and use of lessons learned from previous deployments or engagements to refine their processes.
- Provide past performance examples of its successful delivery of these services.

VAS accreditation is awarded to qualified VAS providers who are capable of providing comprehensive VAS services to operators of classified and unclassified National Security Systems (NSS).

Note: The CIRA and VAS accreditation are part of the Information Assurance Directorate at the National Security Agency (NSA). Information Assurance is responsible for protecting National Security Systems (NSS) - which are systems that handle classified information or are otherwise critical to military or intelligence activities. NSA is granted this authority by National Security Directive (NSD) 42 and subsequently confers authority to IAD to conduct this important mission.
The Directorate works closely with Military Services and Combatant Commands (COCOMs) - particularly United States Cyber Command - to stay abreast of cyber trends and adversarial threats. IAD has developed partnerships with government, industry, and academia in order to commercialize Information Assurance (IA) technology and products. By setting standards and encouraging vendors to build to those standards, IA ensures that secure devices and networks are not only available to customers, but keep pace with current technologies.

IA's objective is to provide Confidence in Cyberspace.

NSA Day of Cyber

- The NSA Day of Cyber is an interactive web platform that enables students to take a seat beside the NSA Cyber Threat Director and test drive a day in the life of six NSA cybersecurity professionals. Students virtually participate in challenging real-world cybersecurity scenarios that will allow them to discover the skills and tools used by the NSA cybersecurity professionals and explore the vast number of careers in cybersecurity. Once completed, each student will each receive their Cybersecurity Resume and Certificate of Completion.
- For more information, click here.

U.S. Department of Defense Advanced Research Projects Agency (DARPA)

- The National Cyber Range is a project overseen by the Defense Advanced Research Projects Agency (DARPA), an agency of the United States Department of Defense responsible for the development of emerging technologies for use by the military. DARPA oversees the National Cyber Range to build a scale model of the Internet that can be used to carry out cyber war games. The project serves as a test range where the military can create antivirus technologies to guard against cyberterrorism and attacks from hackers.
- The 2016 Cyber Grand Challenge (CGC) was a challenge created by DARPA in order to develop automatic defense systems that can discover, prove, and correct software flaws in real-time. The final event was held on August 4, 2016 at the Paris Hotel & Conference Center in Las Vegas, Nevada. The event placed machine versus machine in what is called the "world's first automated network defense tournament."
- The Cyber Grand Challenge corresponded with the 24th DEF CON hacker convention and resembled in structure the computer security game called "capture the flag" that is typically played by groups of humans racing to find a file or secret protected on the other's network. It features, however, a more standardized vulnerability-proving system, in which all exploits and patched binaries are submitted and evaluated by the referee infrastructure. Challenge Binaries run on the 32-bit Intel x86 architecture, albeit with a simplified ABI.
- For more information, click here.
- The tech behind the DARPA Grand Challenge winner, a small Pittsburg-based business called For All Secure, is now being used by the Pentagon. The project is being overseen by thePentagon's startup-centric office, named the Defense Innovation Unit Experimental (DIUx). For All Secure, are the makers of a supercomputer designed to automatically detect, patch and exploit existing software

vulnerabilities, and they were recently awarded a seven-figure contract from the Department of Defense to apply the cutting-edge technology to military systems, including U.S. Navy ships and aircraft. See story here.

U.S. Department of Labor, Bureau of Labor Statistics

The Bureau of Labor Statistics (BLS) is a unit of the United States Department of Labor. It is the principal fact-finding agency for the U.S. government in the broad field of labor economics and statistics and serves as a principal agency of the U.S. Federal Statistical System. The BLS is a governmental statistical agency that collects, processes, analyzes, and disseminates essential statistical data to the American public, the U.S. Congress, other Federal agencies, State and local governments, business, and labor representatives.

The BLS Occupational Outlook Handbook is the government's premier source of career information intended to help job seekers learn about the job market, change jobs, or find information on occupations of interest. It provides information about the nature of the work, education and training requirements, advancement opportunities, employment, salary, and ten-year job outlook for hundreds of occupations. The Handbook also lists related occupations and sources of additional information. The Handbook can help people find career information on duties, education and training, pay, and outlook for hundreds of occupations.

A key issue is that cybersecurity jobs under labor continue categorized under technology.

U.S. General Services Administration (GSA)

The **General Services Administration** (**GSA**), an independent agency of the United States government, was established in 1949 to help manage and support the basic functioning of federal agencies. GSA supplies products and communications for U.S. government offices, provides transportation and office space to federal employees, and develops government-wide cost-minimizing policies and other management tasks.

GSA has an annual operating budget of roughly $26.3 billion. GSA oversees $66 billion of procurement annually. It contributes to the management of about $500 billion in U.S. federal property, divided chiefly among 8,300 owned and leased buildings and a 210,000 vehicle motor pool.

GSA's business lines include the Federal Acquisition Service (FAS), the Public Buildings Service (PBS), and the Technology Transformation Service (TTS), as well as several Staff Offices including the Office of Government-wide Policy, the Office of Small Business Utilization, and the Office of Mission Assurance. TTS's Office of Products and Programs is responsible for five portfolios designed to help federal agencies improve delivery of information and services to the public.

Key initiatives include FedRAMP, Cloud.gov, the USAGov platform (*e.g.*, USA.gov, GobiernoUSA.gov, and Kids.gov), Data.gov, Performance.gov, and Challenge.gov. GSA is member of the Procurement G6, an informal group leading the use of framework agreements and e-procurement instruments in public procurement.

Highly Adaptive Cybersecurity Services (HACS)

GSA has established four (4) Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers (SINs) on IT Schedule 70 to provide agencies quicker access to key, pre-vetted support services that will expand agencies' capacity to test their high-priority IT systems, rapidly address potential vulnerabilities,

and stop adversaries before they impact our networks. The HACS SINs feature high quality cybersecurity vendors offering federal, state, and local governments the following services:

- 132-45A Penetration Testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.
- 132-45B Incident Response services help organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.
- 132-45C Cyber Hunt activities are responses to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunt activities start with the premise that threat actors known to target some organizations in a specific industry, or specific systems, are likely to also target other organizations in the same industry or with the same systems.
- 132-45D Risk and Vulnerability Assessment conduct assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. This SIN offers the following services:
    - Network Mapping
    - Vulnerability Scanning
    - Phishing Assessment
    - Wireless Assessment
    - Web Application Assessment
    - Operating System Security Assessment (OSSA)
    - Database Assessment
    - Penetration Testing

Other Notable Presenters or Organizations

Palo Alto Networks Cybersecurity Academy

The Palo Alto Networks Academy provides degree-granting, accredited academic institutions with courseware, certification, training labs, and faculty training – at no cost – to give today's cybersecurity students hands–on knowledge of the leading next–generation security platform. The will develop train-the-trainer programs, and fully bundled VM-50s/100s for training labs.To sign up, an institution needs to sign the AAC agreement on their public website at www.paloaltonetworks.com/academy, and the Academy team will train faculty and help set up labs—all at no cost to the school. Palo Alto Networks has 275+ Authorized Academy Centers. Last Thursday, Girl Scouts of the USA announced a new partnership with Palo Alto Networks to create a series of cybersecurity badges. The badges, which will be available starting in 2018, can be earned by girls in grades K-12 who demonstrate mastery of Internet security. For the full story, click here.
Palo Alto Networks provides vouchers for certifications.

For a list of the Palo Alto Networks Management Team, click here. GO-Biz CASCADE team should meet with Palo Alto Networks to explore possible alignment on vouchers.

The National Cyber Security Alliance (NCSA)

The National Cyber Security Alliance (NCSA), a 501c(3) nonprofit founded in 2001, is the United States' leading public-private partnership promoting cybersecurity and privacy education and awareness. NCSA works to educate and empower our global digital society to use the internet safely and securely. NCSA coalesces the efforts of the private sector, government and NGOs to engage in far-reaching cybersecurity

awareness efforts and brings together divergent groups in collaborative ways to encourage a culture of cybersecurity and privacy. The executive director is Michael Kaiser. Website: staysafeonline.org.

NCSA's primary partners are the U.S. Department of Homeland Security (DHS) and NCSA's Board of Directors, which includes representatives from ADP; Aetna; AT&T Services, Inc.; Bank of America; Barclays; CDK Global; Cisco; Comcast; ESET North America; Facebook; Google; Intel; LifeLock; Logical Operations; Mastercard, Microsoft Corporation; NXP Semiconductors; PayPal; PKWARE; RSA, the Security Division of EMC; Raytheon; SANS Institute; Symantec; TeleSign; Verizon; Visa; and Wells Fargo.

National Cyber Security Awareness Month

NCSA's core initiatives include the following: National Cyber Security Awareness Month, co-led by NCSA and DHS, provides a platform for industry, government, nonprofits, schools and the public to raise awareness about using the internet and connected devices more safely and securely. NCSA partners with DHS to provide the resources and leadership for the initiative. National Cyber Security Awareness Month (NCSAM) is observed each October since its inception in 2004 in the United States of America.

The official hashtag for the month is #CyberAware.

Data Privacy Day

Data Privacy Day, held annually on January 28, began in the United States and Canada in January 2008 as an extension of Data Protection Day celebrated in the European Union. The theme for the day is "Respecting Privacy, Safeguarding Data and Enabling Trust." The signature event of the year-round data privacy campaign, Data Privacy Day, relies on the broad participation of stakeholders to educate and generate awareness about privacy and data protection through NCSA's free materials and resources. More than 660 organizations and individuals signed up as Champions to support the day in 2017.

The official hashtag for the campaign is #PrivacyAware.

Stop. Think. Connect.

STOP. THINK. CONNECT.™ is the year-round global online safety awareness campaign to help all digital citizens stay safer and more secure online. The research-based messaging was created in 2009 by a coalition of private companies, nonprofits and government with leadership provided by NCSA and the Anti-Phishing Working Group (APWG). DHS provides the federal government's leadership for the campaign. In addition to the original 25 founding companies, more than 680 companies, nonprofit organizations and government entities are official STOP. THINK. CONNECT.™ partners.

American National Standards Institute (ANSI)

The American National Standards Institute (ANSI) is a private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States. The organization also coordinates U.S. standards with international standards so that American products can be used worldwide. ANSI accredits standards that are developed by representatives of other standards organizations, government agencies, consumer groups, companies, and others. These standards ensure that the characteristics and performance of products are consistent, that people use the same definitions and terms, and that products are tested the same way. ANSI also accredits organizations that carry out product or personnel certification in accordance with requirements defined in international standards. ANSI headquarters are in Washington, D.C. and the operations office is located in New York City. The ANSI annual operating budget is funded by the sale of publications, membership dues and fees, accreditation services, fee-based programs, and international standards programs.

ANSI launched a cybersecurity portal in 2015 which features an extensive database of top public- and private-sector resources and provides information on the contributions of ANSI, members of the ANSI Federation, and the broader standardization community to address issues related to cybersecurity. In an effort to provide convenient access to ANSI's various areas of work in support of cybersecurity, the new portal at www.ansi.org/cyber features publications and comprehensive lists of cyber-related resources, including government and private-sector cybersecurity initiatives, ANSI standards packages on IT security, and information on ANSI's conformity assessment activities in this area.

National Council of Information Sharing and Analysis Centers (NCI)

Formed in 2003, the NCI today comprises 24 organizations designated by their sectors as their information sharing and operational arms, also known as Sector-based Information Sharing and Analysis Centers (ISACs). ISACs collaborate and coordinate with each other via the National Council of ISACs (NCI). The NCI is a cross-sector partnership, providing a forum for sharing cyber and physical threats and mitigation strategies among ISACs and with government and private sector partners during both steady-state conditions and incidents requiring cross-sector response. Sharing and coordination is accomplished through daily and weekly calls between ISAC operations centers, daily reports, requests-for-information, monthly meetings, exercises, and other activities as situations require. The NCI also organizes its own drills and exercises and participates in national exercises.

Council members are present on the National Cybersecurity and Communications Integration Center (NCCIC) watch floor, and NCI representatives can embed with National Infrastructure Coordinating Center (NICC) during significant national incidents. The Council and individual members also collaborate with other agencies of the federal government, fusion centers, the State and Local Tribal Territorial Government Coordinating Council (SLTTGCC), the Regional Consortium Coordinating Council (RCCC), the Partnership for Critical Infrastructure Security (PCIS) – the Cross-Sector Council, and international partners.

The Council welcomes membership from organizations that have been designated by their sector leadership as their official forum for sharing threat information. Critical Infrastructure sectors and subsectors that have not yet established a method for sharing across their sectors are encouraged to contact the NCI to discuss how they can collaborate with the Council and participate in its activities.

Website: www.nationalisacs.org/

SANS Institute

The SANS Institute (officially the Escal Institute of Advanced Technologies) is a private U.S. for-profit company founded in 1989 that specializes in information security and cybersecurity training. Topics available for training include cyber and network defenses, penetration testing, incident response, digital forensics, and audit. The information security courses are developed through a consensus process involving administrators, security managers, and information security professionals. The courses cover security fundamentals and technical aspects of information security. The Institute has been recognized for its training programs and certification programs. SANS stands for SysAdmin, Audit, Network and Security.

When originally organized in 1989, SANS training events functioned like traditional technical conferences showcasing technical presentations. By the mid-1990s, SANS offered events which combined training with tradeshows. Beginning in 2006, SANS offered asynchronous online training (SANS OnDemand) and a virtual, synchronous classroom format (SANS vLive). Free webcasts and email newsletters (@Risk, Newsbites, Ouch!) have been developed in conjunction with security vendors. The

actual content behind SANS training courses and training events remain "vendor-agnostic." Vendors cannot pay to offer their own official SANS course, although they can teach a SANS "hosted" event via sponsorship.

NetWars

SANS NetWars is a suite of hands-on, interactive learning scenarios that enable information security professionals to develop and master the real-world, in-depth skills they need to excel in their field. In SANS award-winning courses, attendees consistently rate our hands-on exercises as the most valuable part of the course. With NetWars, we have really raised the ante, as participants learn in a cyber range while working through various challenge levels, all hands-on, with a focus on mastering the skills information security professionals can use in their jobs every day.

NetWars is in use by the US Air Force and the US Army.

CyberTalent Immersion Academy

The SANS Institute has launched a series of scholarship-based Immersion Academies in the U.S for veterans and women. The CyberTalent Immersion Academy is an intensive, accelerated training program that provides SANS world-class training and GIAC certifications (learn about GIAC below) to quickly and effectively launch careers in cybersecurity. A number of other organizations and employers have launched new workforce development and apprenticeship programs to grow the cybertalent pool as well. The SANS various pipeline talent development programs are intended to continue to bring new individuals into cybersecurity on a larger scale and make a dent in the workforce shortage.

Global Information Assurance Certification (GIAC)

GIAC (Global Information Assurance Certification) was founded in 1999 by the SANS institute to validate the skills of information security professionals. The purpose of GIAC is to provide assurance that a certified individual has the knowledge and skills necessary for a practitioner in key areas of computer, information and software security. GIAC certifications address a range of skill sets including entry-level information security and broad-based security essentials, as well as advanced subject areas like: Audit, Intrusion detection, Incident handling, Firewalls and perimeter protection, Forensics, Hacker techniques, Windows and Unix operating system security, Secure software and application coding. GIAC Certifications develops and administers premier, professional information security certifications. More than 30 cyber security certifications align with SANS training and ensure mastery in critical, specialized InfoSec domains. GIAC Certifications provide the highest and most rigorous assurance of cyber security knowledge and skill available to industry, government, and military clients across the world. GIAC certifications measure specific skills and knowledge areas (versus general infosec knowledge). GIAC offers the only certifications that cover advanced technical subject areas. GIAC certifications are valid for four years. Students must review new course information and retake the exams every four years in order to remain certified. Different education and certification tracks are available for the following categories:

- Cyber Defense
- Penetration Testing
- Incident Response and Forensics
- Management, Audit, Legal
- Developer
- Industrial Control Systems

- GIAC Security Expert (GSE)

Booz Allen Hamilton

National Security Cyber Assistance Program

Booz Allen Hamilton Inc. (informally: Booz Allen) is an American management consulting firm, sometimes referred to as a government-services company, headquartered in McLean, Virginia. It has 80 other offices around the globe. Booz Allen holds three U.S. Government's elite cybersecurity accreditations: the National Security Agency's Cyber Incident Response Assistance (CIRA) accreditation, the NSA's Vulnerability Assessment Service (VAS) accreditation, and the General Services Administration's Highly Adaptive Cybersecurity Services schedule. Booz Allen is recognized as an independent trusted agent of the Air Force Enterprise and Space Security Control Assessor as a licensed Agent of the Security Control Assessor (ASCA).

CyberSeek

The CyberSeek interactive map allows the user to view information about cybersecurity supply and demand by state or metro area. Cyberseek aims to deliver a vast amount of valuable information on where the security jobs are, how to get them, what career tracks are available and how much money people can expect once they are hired. Cyberseek has two primary components: One is a comprehensive analytics tool detailing supply and demand for cybersecurity jobs and the other is a career pathway aimed to teach job seekers how to map out the next steps toward a career in cybersecurity.

During the NICE 2017 conference, it was announced that several new features have been added to CyberSeek to provide greater visibility into the supply and demand of cybersecurity workers at the national, state, and metropolitan levels. One key new feature of the CyberSeek heat map is the ability to track data on cybersecurity job demand overall and within the public and private sectors. The CyberSeek career pathway, which maps to the NICE Cybersecurity Workforce Framework, has also been enhanced to help both individuals interested in cybersecurity careers and employers looking to fill job openings. The expanded, interactive career pathway includes information on 10 core cybersecurity roles and 5 tech jobs that often serve as "feeder roles" to cybersecurity positions.

The updated site also includes an embeddable heat map and career pathway widgets. Anyone interested in the cybersecurity workforce can embed versions of the heat map and career pathway on their websites with links back to CyberSeek.org.

CyberSeek is linked to the CAE community via search function.

Cyberseek is backed by the National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), the Computing Technology Industry Association (CompTIA), and Burning Glass Technologies.

Burning Glass Technologies

Burning Glass Technologies is a Boston-based company that specializes in job matching and labor market analytics solutions for the education and workforce sectors. Their technologies analyze millions of job postings from more than 40,000 sources, providing educators with real-time intelligence on skills in demand to inform program design and expansion, employer outreach, and career services. It is ultimately an analytics software company powered by the world's largest and most sophisticated database of labor market data and talent. They deliver real-time data and planning tools that inform careers, define academic programs, and shape workforces.

For more information, contact Stephen Lynch, Director of Workforce & Economic Development Services at slynch@burning-glass.com or (617) 227-4800.

CompTIA

The Computing Technology Industry Association (CompTIA) is a non-profit trade association that issues professional certifications for the information technology (IT) industry. It is considered one of the IT industry's top trade associations. Based in Downers Grove, Illinois, CompTIA issues vendor-neutral professional certification in over 120 countries. The organization releases over 50 industry studies annually to track industry trends and changes. Over 2.2 million people have earned CompTIA certifications since the association was established.

Cybersecurity Career Pathway

The CompTIA Cybersecurity Career Pathway helps IT pros achieve cybersecurity mastery, from beginning to end. The centerpiece is the CompTIA Security+ certification. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. After earning CompTIA Security+, cybersecurity professionals can take the next step by pursuing CompTIA Cybersecurity Analyst (CSA+), which assesses three to four years of cybersecurity field work. After CompTIA CSA+, IT pros can pursue CompTIA Advanced Security Practitioner (CASP), to prove their mastery of cybersecurity skills required at the 5- to 10-year experience level.

San Diego Cyber Center Of Excellence (CCOE)

During the NICE 2017 conference, RADM Ken Slaght led a session on Aligning Academic Supply and Industry Demand. Key take-aways:

1. It is becoming increasingly clear that existing Cybersecurity growth, leadership and development of workforce has been primarily happening from a bottom-up approach via regional Cybersecurity eco-system pockets like San Diego (vs. via top-down federal/state government or industry approach).
2. It is challenging to keep locally educated cyber talent in these regional economies (quickly poached by Silicon Valley/Maryland).
3. The San Diego cybersecurity eco-system model, particularly re workforce training and development, is one that could be strategically replicated/tailored to other areas of California.

RADM Ken D. Slaght, USN (ret.) is the Co-Chair and President of the San Diego Cyber Center Of Excellence (CCOE), a non-profit dedicated to accelerating the region's cyber economy and positioning it as a global hub of cyber innovation. After retiring from the U.S. Navy at the rank of Rear Admiral, Slaght worked as VP of General Dynamics Information Technology. Prior to that, he was the commander of the Space and Naval Warfare Systems Command (SPAWAR). During his naval career, Slaght served as commander of the ammunition ship USS Flint and served tours as executive officer aboard several other ships. Slaght also sits on the California Governor's Military Council.

Slaght shared the results of the CCOE's San Diego Cybersecurity Industry Economic Impact Analysis and Workforce Study, June 2016. San Diego has been on a three-year effort to build a cluster of expertise around cybersecurity, and it is taking root with an estimated 14.7% increase in cyber jobs since the San Diego Regional EDC's 2014 Cybersecurity in San Diego: An Economic Impact and Industry Assessment. Given San Diego's commitment to growing its cyersecurity ecosystem, 7,620 direct jobs and 16,580 total jobs have been impacted in San Diego. However, it Slaght explained that it has been challenging to keep locally educated cyber talent in the region. Currently San Diego is losing almost 75% to Silicon Valley and Maryland (NSA). To address this, the CCOE has established a local cyber jobs board, initiated campus visits by local cyber company leadership, and energized cyber internships/apprenticeships. A key

success factor for San Diego has been the collaborative Cybersecurity ecosystem approach that includes industry, academic and government institutional will. CCOE was founded by a collection of world-class cyber companies with operations in San Diego (e.g. Sentek Global, ESET, Qualcomm, FICO, Lockton Insurance, Morrison Foerster, San Diego Regional EDC and the United States Navy's Space and Naval Warfare Systems Command (SPAWAR). The City of San Diego has also had the political will and ability to support Cybersecurity ecosystem growth. These are all important ingredients in establishing a Cybersecurity ecosystem recipe.

The San Diego model is one that could be strategically replicated/tailored to other areas of California. GO-Biz and CASCADE should engage the CCOE in statewide outreach and other higher-level policy/legislative efforts, potentially in collaboration with other CASCADE grantees and the Cal Poly SLO/GO-Biz cyber effort.

Please click here for Ken Slaght's presentation.

California State University, San Bernardino (CSUSB)

California State University, San Bernardino (CSUSB) had a significant presence in the conference, with several faculty members and students from the Cyber Security Center present. CSUSB has been designated as a Center of Academic Excellence in Information Assurance by the National Security Agency and the Department of Homeland Security since 2008. CSUSB was also just designated as a Center of Academic Excellence in Cyber Defense/Information Assurance through 2021. They are further recognized in specialty areas in Cyber Investigations and Network Security Administration. Business Administration with a Cyber Security concentration was one of the first cyber security tracks in California. CSUSB now has expanded their Cyber curriculum to include Criminal Justice, Public Administration, and National Security Studies. The CSUB Information and Decisions Sciences (IDS) department has received cyber security grants from the National Science Foundation, Department of Defense, and other federal and state agencies. From their award-winning Cyber Defense teams to well-equipped cyber security lab, CSUSB is a model academic cyber institution. Dr. Tony Coulson is the Director of the CSUSB Cyber Security Center: tcoulson@csusb.edu, (909) 537-5768.

In addition, CSUSB Institute of Applied Research (IAR) and the CSUSB Inland Empire Center for Entrepreneurship (IECE) are grantees of the U.S. Department of Defense California Advanced Supply Chain and Diversification Effort (CASCADE), an initiative funded by the U.S. Department of Defense to bolster California's defense supply chain cybersecurity resilience, innovation capacity and diversification strategies, and to support the growth and sustainment of California's Cybersecurity workforce through cybersecurity-related education curricula, training and apprenticeship programs.

CASCADE Cyber Supply Chain Mapping and Analysis Component

Under the CASCADE program, the Institute of Applied Research (IAR) at California State University San Bernardino is leading a supply chain mapping project that will help to identify the communities, businesses and workers that may be affected by changes in defense spending. Mapping of California's overall defense supply chain is the major focus of the project. However, a key minor focus is gaining an understanding of the capacity of California's cyber firms and mapping California's cyber supply chain, in order to assist with defense contractor modernization and diversification. The mapping process will identify firms (including large defense contractors as well as small and medium-sized manufacturers in the supply chain) that may be at risk due to reduced defense contracting and procurement. These firms are integral to the economic health of the state as a whole. Further, the specific workforce development needs to be addressed by other project partners (i.e. capacity building for cybersecurity skills development) can best be determined with a clear understanding of which industries and firms are at risk (which is one

outcome of the mapping process). Identifying and mapping the supply chain is a necessary first step towards helping companies mitigate the negative effects of defense cutbacks by successfully transitioning to new opportunities. IAR will be involved in developing the methodology for the data gathering process and for helping to coordinate a statewide strategy to accomplish the study tasks in cooperation with other project partners. The methodology and strategy developed in this study will provide a template which can be used across sectors.

CASCADE Entrepreneurial and Business Skills Development

The Inland Empire Center for Entrepreneurship (IECE) at California State University San Bernardino (CSUSB) is providing intensive entrepreneurial training that will prepare current displaced defense industry workers for potential opportunities of self-employment as entrepreneurs. In addition, the proposed training will also prepare participants to be more innovative, business-oriented and entrepreneurial employees should they choose not to pursue self-employment options. Using a modular, experiential learning curriculum derived from CSUSB's nationally recognized entrepreneurship degree program, IECE will deliver a 10-week course (40 hours) that will prepare individuals to understand the basics of business ownership, what constitutes the entrepreneurial experience, the process of creating a new business venture, assessing the feasibility of business concepts, accessing critical resources, financial management and developing a business plan. Upon completion, each participant will have a better understanding of their entrepreneurial potential and the process of developing and launching a new venture. Depending on the targeted area, the curriculum can be adjusted to match the skills/background of the participants. As an example, for engineers and technology oriented professional positions, the curriculum includes additional elements such as technology commercialization and intellectual property. The California Workforce Development Board has certified this project. The director of the CSUSB Inland Empire Center for Entrepreneurship is Mike Stull. He is also the Chair of the Department of Management, College of Business & Public Administration. Phone: (909) 537.3708, Email: mstull@csusb.edu.

It will be important for CA Governor's Office to better understand the internal CSUSB strategic alignment as it relates to the State of California's new Cyber program, CASCADE.

Cal Poly San Luis Obispo California Cyber Training Complex (CCTC)

The Cyber Training Complex at Cal Poly San Luis Obispo was often mentioned as a model throughout side discussions during the NICE conference. A recognized leader in cybersecurity education, the university has two cyber labs, faculty and multiple partnerships with industry– crucial elements for workforce development and research.

The California Cyber Training Complex (CCTC) at Cal Poly San Luis Obispo is a robust, multi-agency effort to protect California through enhanced cybercrime forensics and state-wide tactical response training. As an extension of Cal Poly's Cybersecurity Center, the CCTC aims to educate the next generation cyber workforce and provide faculty and students with a new, hands-on research and learning environment.

Camp San Luis Obispo provides critical infrastructure. Situated on California's scenic central coast, it is the ideal location to host the California Cyber Training Complex. Multiple federal, state and local agencies already train thousands of first responders onsite annually and the complex is the home to the California National Guard's Cyber Protection Team. Camp San Luis Obispo also sits on the second largest fiber hub in the U.S., which allows for high bandwidth communication and collaboration on data intensive problems.

The CCTC includes the following facilities:

Cyber Academic Training Center

A state-of-the-art training and lecture facility that emphasizes hands-on cybersecurity and cyber forensics training.

Cyber Test Range and Experimental Laboratory

A 100,000 square-foot facility to develop nextgeneration cyber forensics techniques and tactics, and simulate adversarial cyber activities during training exercises.

Central Coast Forensics Lab (CCFL)

A joint task force of cyber forensic experts drawn from across California will collaborate and share best practices in this state-of-the-art cyber forensics facility.

Cyber Crime Field Training Complex (FTX)

A field training facility to simulate active crime scenes use to develop, test, and train cybercrime prosecution tactics and techniques.

The CCTC serves as an extended Learn by Doing space for Cal Poly students, where they can explore new cyber technologies and train and test tactics side-by-side law enforcement professionals and cyber forensics experts. The program offers an environment for cyber defense innovation through advanced study and basic and applied research on emerging issues and technical challenges, helping to shape California's cyber standards and practices.

California Cyber Innovation Challenge (CCIC)

The California Cyber Innovation Challenge (CCIC) is the state-level cyber security championships sponsored by the California Governor's Office of Business and Economic Development (Go-Biz). Cal Poly and the California Cyber Training Complex (CCTC) have been selected as the host of the CCIC for 2017 and 2018.

The CCIC will feature two competitions, a CyberPatriot-like event and a Digital Forensics Challenge (DFC). CyberPatriot (CP) is a well-established cyber security competition where students are given a drive image and have to fix vulnerabilities in this drive image. The DFC event is influenced by the CCTC's initial training directive of supporting cyber training for law enforcement and the national guard. The DFC will require competitors to seize and search digital devices to put together a criminal case and defend that case to a judge.

For more information on the California Cyber Training Complex (CCTC), please visit. Bill Britton is the VP, CIO and Director of the Cybersecurity Center, bibritto@calpoly.edu, (805) 756-2190. James Baker is the Director for Industry Outreach for the CCTC ITS, jbaker30@calpoly.edu, (805) 756-2948.

About CASCADE

The California Advanced Supply Chain Analysis & Diversification Effort (CASCADE) is an initiative funded by the U.S. Department of Defense to bolster California's defense supply chain cybersecurity resilience, innovation capacity and diversification strategies, and to support the growth and sustainment of California's Cybersecurity workforce through cybersecurity-related education curricula, training and apprenticeship programs.

CASCADE is being led by the California Governor's Office of Business and Economic Development (GO-Biz) and the California Governor's Office of Planning and Research (OPR). The CASCADE program includes 15 funded projects in partnership with government, industry, community, and academic institutions. Partner CASCADE project activities include cyber labor market research, cyber industry convenings, cyber provider surveys, , supply chain mapping, supply chain outreach and resilience workshops, cyber physical security assessments, innovation and commercialization programs. The fundamentals of the projects will revolve around cybersecurity provider, defense supply chain and cyber workforce: (a) Research and analysis, (b) Education and outreach, (c) Standards frameworks and best practices, (c) Innovation, commercialization and diversification, (d) Assistance and development programs.

One of the key relevant CASCADE projects as it relates to NICE is what U.S. Department of Defense and the State of California call "Project 2: Cybersecurity Labor Market Analysis".

CASCADE Cybersecurity Labor Market Analysis

Through CASCADE, the California Community Colleges Centers of Excellence for Labor Market Research (COE) is conducting cybersecurity labor market analysis. This labor market analysis will include both a workforce demand analysis and a workforce supply analysis. The COE workforce demand analysis will include the cybersecurity workforce needs of defense supply chain businesses. This demand study will help identify cybersecurity skills gaps, serve as a resource for changes in community college curriculum, and build capacity in cybersecurity workforce development. This study will also help potentially displaced defense workers identify cybersecurity job openings and training programs applicable to a variety of advanced technology industries.

John Carrese is the Director of the California Community Colleges Centers of Excellence for Labor Market Research hosted at City College of San Francisco. Phone: (415) 452-5529, Email: jcarrese@ccsf.edu The Center is one of seven regional Centers of Excellence funded by the Chancellor's Office of the California Community Colleges. Mr. Carrese implements the Center's environmental scanning, partnership development and technical assistance activities on behalf of the 28 community colleges in the Bay Area. He has authored numerous environmental scan reports on industries such as Information and Communications Technologies, Health, Biotechnology and has collaborated with Lawrence Berkeley National Lab on a study of the workforce needs of energy efficiency employers in California. Mr. Carrese has over 25 years of experience in the workforce and economic development field and has worked at City College of San Francisco for the past 18 years. He is skilled in designing and evaluating performance-based training programs, as well as facilitating project teams. He is also an experienced facilitator of the DACUM (Developing a Curriculum) process with industry and college partners.