



**ECONOMIC &
WORKFORCE
DEVELOPMENT**
through the
CALIFORNIA
COMMUNITY
COLLEGES

**BUSINESS AND WORKFORCE
PERFORMANCE IMPROVEMENT INITIATIVE**



**Environmental Scan Report
Los Angeles County**

CYBERSECURITY

**“Information, Computers, Networks
and Internet Security”**



Center of Excellence

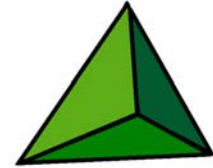
Hosted at Mt. San Antonio College

July 2007



**ECONOMIC &
WORKFORCE
DEVELOPMENT**
through the
CALIFORNIA
COMMUNITY
COLLEGES

**BUSINESS AND WORKFORCE
PERFORMANCE IMPROVEMENT INITIATIVE**



Environmental Scan for Los Angeles County Community Colleges

CYBERSECURITY

July 2007

Prepared By:

Center of Excellence
Serving Los Angeles County
Hosted at Mt. San Antonio College
1100 N. Grand Ave., Building 35, Walnut, CA 91789
Phone: (909) 564-5611, ext. 6106 Fax: (909) 468-4093
areille@mtsac.edu
www.ccewd.net

In collaboration with:

Godbe Research
785 Grand Avenue, Suite 200, Carlsbad, CA 92008
Phone: (760) 730-2944 Fax: (760) 720-4706

THE BUSINESS AND WORKFORCE PERFORMANCE IMPROVEMENT INITIATIVE IS FUNDED IN PART BY THE CHANCELLOR'S OFFICE, CALIFORNIA COMMUNITY COLLEGES, ECONOMIC AND WORKFORCE DEVELOPMENT PROGRAM. THE TOTAL GRANT AMOUNT (GRANT NUMBER 06-305-016 FOR \$205,000) REPRESENTS COMPENSATION FOR MULTIPLE DOCUMENTS OR WRITTEN REPORTS THROUGH THE CENTERS OF EXCELLENCE.

OUR MISSION IS TO STRENGTHEN CALIFORNIA'S WORKFORCE AND ADVANCE ECONOMIC GROWTH THROUGH EDUCATION, TRAINING AND JOB DEVELOPMENT.

Table of Contents

Executive Summary	4
Introduction	5
Labor Market	5
Employers	5
Occupations	5
Demand	7
Occupational Skills and Training Requirements	8
Industry Validation	10
Existing Programs	11
Community Colleges in Los Angeles County	11
Model Programs Out-of-State	12
Other Training Providers	12
Implications and Recommendations for Community Colleges	13
Conclusion	14
References and Resources	15
APPENDIX A: How to Utilize this Report	16

EMPLOYERS ACROSS INDUSTRIES NEED INFORMATION TECHNOLOGY EMPLOYEES WITH EXPERTISE IN CYBERSECURITY. THOSE JOBS OFFER ATTRACTIVE WAGES AND ARE EXPECTED TO GROW BY 18.5% BETWEEN 2002 AND 2012 TO REACH 106,220. – Source: California Employment Development Department

Executive Summary

Advances in information technology allow people to conduct business online, purchase goods and services, manage their money and conduct all manner of business transactions online. More and more industries have changed the way they do business by integrating cutting-edge information technology, and they must protect themselves and their customers against unauthorized access to sensitive information and potential damage to systems caused by viruses and worms.

As a result, the demand for employees with cybersecurity expertise is increasing rapidly and employers are facing a shortage of qualified workers. According to the California Employment Development Department (EDD), in 2012 Los Angeles County will have 106,220 information technology jobs requiring varying degrees of information security and network security expertise. These high-demand jobs offer competitive wages and promotion opportunities.

Cybersecurity education or training from the community colleges can lead to employment in the following positions: IT Security Analyst, Network Security Technical Specialist, IT Security Administrator, Information Security Manager or Data Security Analyst. Students who continue their education, obtain at least a four-year degree, and gain work experience can become Managers, Administrators or Engineers in Network Security, Software Security or Database Security.

Organizations such as the American Association of Community Colleges (AACC) have studied and documented the need for training and education from Community Colleges in the area of cybersecurity. In addition, for the purpose of this study, an employer survey was conducted by Godbe Research to validate workforce development needs specific to Los Angeles County. Thirty businesses employing information technology staff participated in a 25-minute phone interview. Seventy percent of respondents indicated that they had either “Great difficulty” or “Some difficulty” recruiting information security employees, both at the entry level and advanced level.

The community colleges have an opportunity to provide training and education in the area of cybersecurity to traditional students and incumbent workers to keep their skills current. It is critical for the colleges to collaborate with employers, to make students work on real case studies, to remain up-to-date and to effectively market the courses to avoid low-enrollment. Businesses are willing to work with educational institutions and donate resources, but colleges have to demonstrate their ability to be responsive and flexible, to meet employers’ needs.

Introduction

The considerable progress made in information technology has revolutionized nearly all industries, as well as many aspects of our lives, but it has also created vulnerability. The downside of technology is the threat posed by viruses, worms and unauthorized access to information (both business and personal information). The Computer Security Institute's 2002 Computer Crime and Security Survey¹ of large corporations and government agencies revealed that:

- 90 percent of respondents had detected computer security breaches;
- 80 percent of respondents had suffered financial losses as a result of computer breaches;
- 85 percent of respondents had detected computer viruses.

People use the internet to shop, pay bills, transfer funds, open accounts, access health records, make doctors appointments and access information on their accounts with almost any organization with which they conduct business. The convenience is invaluable for customers, but businesses must ensure that personal information is secure. Consequently, the need for trained employees in the area of cybersecurity is increasing rapidly, and the trend is expected to continue as technology allows more and more operations to be conducted virtually.

Cybersecurity is not an industry, but a component of business operations across industries. The workforce can be defined as including any occupation that protects networks and electronic information systems from unauthorized access to sensitive information. Employee responsibilities include ensuring the integrity of data, implementing appropriate privacy standards for information, and protecting information systems from external sources that attempt to disrupt the functionality of the network.

Labor Market

Employers

Workers skilled in the area of cybersecurity may work for virtually any employer across sectors such as banking, financial services, e-business, software or hardware manufacturers, information technology-related services, law-enforcement, health care, government, education, or even hospitality and tourism.

Occupations

Cybersecurity occupations include²:

¹ Richard Power, "2002 CSI/FBI Computer Crime and Security Survey." Computer Security Issues and Trends, vol. 8, no. 1 (Spring 2002). Available online at www.gocsi.com

² "Computer and Information Security Labor Market Study", June 2006, Godbe Research.

- **IT Security Analyst:** Provides critical input throughout the project management lifecycle to protect information systems and critical data from violations of policy, regulations, or customer expectations as they relate to confidentiality, integrity, availability, and delivery of security certification.
- **Network Security Technical Specialist:** Implements systems for customer requirements, providing support in client environments, ensuring customer expectations are met.
- **IT Security Administrator:** Provides user account administration and support for all network based resources, as well as responsibility for developing secure client directories and other information classification and protection initiatives.
- **Information Security Manager:** Assists in creating and maintaining security for all Systems Applications and Products (SAP) authorizations, profiles and roles. Translates business requirements into SAP security roles. Leads in design, configuration and testing of security activities. Monitors and certifies users and security profiles on a periodic basis.
- **Data Security Analyst:** Assures that computing infrastructure and applications meet information security best practices and comply with regulations for information security.
- **Application Security Engineer:** Designs and Implements security technologies including reverse proxy, firewall and server level policy agents. Develop detailed risk assessments, security plans and risk mitigation plans to identify and mitigate risks.
- **Network Security Engineer:** Configures, maintains and monitors firewalls, intrusion detection systems (IDS), and routers, as well as incident response and management activities.
- **Security Software Engineer:** Develops, enhances and maintains security software sold to customers and business partners.
- **Security Sales Engineer:** Prepares and provides configurations and pricing on standard, complex and special hardware and applications, prepares responses to the technical sections of RFP's/RFQ's and conducts technical sales presentations.
- **Database Security Engineer:** Serves as technical lead and conducts database security risk assessments, architectural reviews, security analysis and evaluation of enterprise networks.

IT Security Analyst, Network Security Technical Specialist, IT Security Administrator, Information Security Manager or Data Security Analyst positions can be filled with community college graduates. Students who continue their education, obtain at least a four-year degree, and gain work experience, can become Managers, Administrators or Engineers in Network Security, Software Security or Database Security.

Demand

Information security occupations do not have specific occupational codes and thus are not tracked separately from other information technology occupations, but are included in the job categories listed in the next table.

According to EDD, both median hourly wages and job growth rates are significantly higher for jobs in information technology requiring cybersecurity expertise than for the average of all occupations in Los Angeles County. IT security occupations are in high demand and pay high wages. The fastest growing occupations are Network Systems and Data Communications Analysts, Database Administrators, Computer Systems Analysts, Computer and Information Systems Managers, Computer Software Engineers and Computer Support Specialists.

Occupational Employment Projections* 2002-2012

Los Angeles County

SOC Code	Occupational Title	Annual Average Employment		Employment Change		Median Hourly Wage [1]
		2002	2012	Numerical	Percent	
00-0000	All Occupations (total labor force)	4,026,800	4,485,500	458,700	11.4	\$14.93
	Information Technology (IT) Occupations:					
11-3021	Computer and Information Systems Managers	7,520	9,130	1,610	21.4	\$49.83
15-1011	Computer and Information Scientists, Research	360	410	50	13.9	\$51.64
15-1021	Computer Programmers	9,660	9,490	-170	-1.8	\$34.16
15-1031	Computer Software Engineers, Applications	18,060	20,910	2,850	15.8	\$39.83
15-1032	Computer Software Engineers, Systems Software	7,240	8,770	1,530	21.1	\$40.72
15-1041	Computer Support Specialists	14,960	17,810	2,850	19.1	\$20.24
15-1051	Computer Systems Analysts	11,940	14,740	2,800	23.5	\$32.75
15-1061	Database Administrators	3,480	4,350	870	25.0	\$32.42
15-1071	Network and Computer Systems Administrators	8,420	10,180	1,760	20.9	\$30.35
15-1081	Network Systems and Data Communications Analysts	3,810	5,310	1,500	39.4	\$28.56
15-1099	Computer Specialists, All Other	4,210	5,120	910	21.6	\$33.34
	Totals:	89,660	106,220	16,560	18.5	

Source: Employment Development Department <http://www.labormarketinfo.edd.ca.gov/>

* March 2003 Benchmark

Occupation subtotals may not add to the totals due to rounding and the suppression of data.

[1] Median Hourly Wage is the estimated 50th percentile of the distribution of wages; 50 percent of workers in an occupation earn wages below, and 50 percent earn wages above the median wage. The wages are from the first quarter of 2005.

Data from Economic Modeling Specialists, Inc.³ (EMSI), formerly known as CC Benefits, Inc., also shows job growth and high wages; however, the number of jobs given for 2007 is greater than EDD's projections for 2012. The two data sources indicate different job growth rates by occupation, but both suggest that all occupations will grow, with the exception of Computer Programmers. According to EMSI, the fastest growing occupations are Network Systems and Data Communications Analysts, Computer Software Engineers, Network and Computer Systems Administrators and Database Administrators.

Occupational Employment Projections 2007-2017

Los Angeles County

SOC Code	Description	2007 Jobs	2017 Jobs	Absolute change	% change	Hourly Wages
11-3021	Computer and Information Systems Managers	10,897	12,153	1,257	12%	\$49.38
15-1011	Computer and Information Scientists, Research	1,827	1,856	29	2%	\$39.17
15-1021	Computer Programmers	14,146	12,518	-1,628	-12%	\$29.80
15-1031	Computer Software Engineers, Applications	23,276	28,774	5,498	24%	\$40.24
15-1032	Computer Software Engineers, Systems Software	10,277	12,144	1,867	18%	\$38.26
15-1041	Computer Support Specialists	18,925	20,312	1,387	7%	\$19.06
15-1051	Computer Systems Analysts	16,911	19,215	2,304	14%	\$30.78
15-1061	Database Administrators	4,054	4,903	850	21%	\$31.52
15-1071	Network and Computer Systems Administrators	9,826	12,036	2,210	22%	\$28.85
15-1081	Network Systems and Data Communications Analysts	8,954	11,269	2,316	26%	\$26.96
15-1099	Computer Specialists, All Other	5,704	5,829	125	2%	\$32.91
	Total	124,795	141,009	16,213	13%	\$32.69

Source: Economic Modeling Specialists, Inc. 7/2007

Occupational Skills and Training Requirements

The American Association of Community Colleges was awarded a National Science Foundation grant, which funded a thorough study of the role of community colleges in cybersecurity education. As a result, a report⁴ was published which listed job requirements including:

1. General Security Issues

- Survey of computer security literacy issues, awareness, and ethics.

³ Economic Modeling Specialists, Inc.: www.economicmodeling.com

⁴ Protecting Information: The Role of Community Colleges in Cybersecurity Education. American Association of Community Colleges. June 2002.

- Host security and scope of security in relation to today's technologies.
- Confidentiality, integrity, availability, authentication, authorization, and non-repudiation.
- Personal and corporate privacy issues.
- TCP/IP (Transmission Control Protocol/Internet Protocol).

2. Business and Economic Issues and Security Policies

- Business and institutional structures, strategies, and policies.
- Vulnerability, threats, acceptable risk, and risk mitigation (including knowledge of an established taxonomy and an established trusted system for evaluation like the Information Technology Security Evaluation Criteria (ITSEC)).
- Management of risk, including risk control, reduction of risk, avoidance of risk, assumption of risk, active defense, and transfer of risk (chain of trust agreements, insurance underwriting, warranties).

3. Law, Ethics, and Standards

- Federal, state, local and international laws.
- Legal implications of security measures and breaches.
- Ethical aspects of cybersecurity.
- Legal and regulatory aspects, including understanding of the judicial system, investigative processes, evidence chain, and incident reporting. What should be reported, and to whom.
- Forensics guidelines and protocols.

4. General Knowledge and Skills

- Telecommunications and strong technological foundation.
- Customer relations.
- Strong verbal and writing skills, including levels of techno-speech.
- Management ability.
- Strategic and tactical thinking.
- Creativity.

5. Internet and Cybersecurity Skills and Knowledge

A. Software, Hardware, and Operating Systems

- Strong technical knowledge of hardware and software.
- Cryptography.
- Programming.
- Application knowledge.

B. Network Security

- Networks in telecommunications network security; for example, knowledge of networks, servers, systems, databases, signaling networks and gateways, network and element management systems, and network elements.
- Basic network security, information security, database security, system security, communications security, etc.

C. Security Protocols

- Confidentiality, integrity, availability, authentication, authorization, non-repudiation, and privacy.
- Basic security standards for software development.
- Strong authentication and secure credentials exchange.
- Fluency with firewalls and firewall installation.
- Antivirus, anti-Trojan horse, scanning, and backup.

D. Threat Management

- Identifying threats.
- Access and environmental management requirements.
- Policy and procedures security development.
- Knowledge of historical exploits.

For a complete list, please refer to the AACC report available at:

http://www.aacc.nche.edu/Content/NavigationMenu/ResourceCenter/Projects_Partnerships/OtherInitiatives/Cybersecurity/Cybersecurity.htm

Industry Validation

The Center of Excellence worked with Godbe Research on a survey to validate the need in Los Angeles County for workers trained in the area of cybersecurity. A list of companies was created from the InfoUSA database, with 100 businesses working in the information technology cluster and 801 large businesses in various industries employing information technology staff. All employers were located within Los Angeles County. Of the 901 businesses contacted, 30 agreed to participate in a 25-minute telephone interview. The survey report highlights were:

- **Demand for employees is high and growing:** Seventy percent (70%) of respondents indicated that they had either “Great difficulty” or “Some difficulty” recruiting information security employees, both at the entry level and advanced level. In Los Angeles County, the demand for permanent employees in information security is expected to increase by approximately 9% over the next 12 months, while the demand for temporary employees is expected to increase by around 21%⁵.
- **Only half of positions are filled from within:** Fifty percent (50%) of companies reported that they typically recruited new hires from outside the firm for cybersecurity positions, when a non-entry level position became available. Also, 20% stated that they always or frequently recruited individuals from outside Los Angeles County, and 7% frequently recruited from outside Southern California.
- **Firms show high levels of commitment to employee training:** The survey found that the most popular employee development practice for the occupations considered was informal on-the-job training, which was utilized by 87% of responding companies.

⁵ “Computer and Information Security Labor Market Study”, June 2006, Godbe Research.

By comparison, 67% utilized employer-paid outside training, 57% used formal on-the-job training and in-house classroom training, 43% made use of internship or mentorship programs, and 37% offered tuition assistance. In general, information security employers revealed a stronger commitment to internal training and employee development than found in other comparable clusters.

- **Employment growth is expected:** According to the survey, the two occupations that are expected to have large growth over the next year are Database Security Engineer and Data Security Analyst. The occupations with the highest expected turnover rates are Information Security Manager and IT Security Administrator.
- **Firms have difficulty hiring:** Respondents had the most difficulty finding qualified applicants for the following occupations: Information Security Manager, IT Security Administrator and Network Security Technical Specialist. Employers most often recruited IT Security Administrators from outside of the Los Angeles County area.

Moreover, the need for community colleges to address the workforce issue was further confirmed by businesses serving on colleges' information security programs' advisory committees. They expressed their support by donating time and equipment, and partnering on grant applications. They were eager to work with community colleges that can be flexible and responsive, update programs, customize classes, and provide quality education at an affordable cost. They also recommended that colleges make their courses transferable to universities, and encourage students to continue their education.

Existing Programs

Community Colleges in Los Angeles County

Training and education from the community colleges in Los Angeles County range from individual courses to certificate programs and degree programs as presented below:

Cerritos College

Cyber Security Certificate of Completion, 17 units, 5 classes:

- Network Fundamentals
- Wireless Network
- Network Security Fundamentals
- Special Topics in Security
- Microsoft Windows Security

Glendale College

- Workstation Security & Support, 3 units
- Advanced Networking: Security, 3 units

Long Beach City College

- Introduction to Information Security, 1 unit
- Network Security Certification

Los Angeles City College

- UNIX System Security, 3 units

Los Angeles Trade Tech

- IT Security Specialist Level I Certificate

Mt. San Antonio College

- Computer Network Administration & Security Management A.S. Degree, 29 units
- CIS Professional Certificate in Network Security, 12 units

Note: Mt. SAC has a Regional Information Systems Security Center (RISSC⁶).

Santa Monica College

- Security in VB.NET Applications, 3 units
- Secure Server Installation & Administration, 3 units

Colleges have varying levels of enrollment, program success and involvement with businesses. It is crucial for colleges to keep up-to-date because the knowledge and skills required for information security are expanding extremely rapidly.

Model Programs Out-of-State

Robert D. Campbell, from Rock Valley College in Illinois, and Elizabeth K. Hawthorne, from Union County College in New Jersey, conducted a study of various approaches to cybersecurity education by five community colleges:

- Seminole Community College (Florida)
- Northern Virginia Community College (Virginia)
- The Community College of the Air Force (Alabama)
- Edmonds Community College (Washington)
- Roane State Community College (Tennessee)

The different approaches are:

- A four-semester Associate Degree
- A two-semester Certificate Program
- A course in Cybersecurity
- A non-credit Industry Certification

These model programs were contacted to obtain current information on the programs' success and best practices or recommendations to other colleges. Seminole Community College reported a moderate success and flat enrollment, while Edmonds Community College (EdCC) reported outstanding enrollment, retention rate and completion rate. EdCC was able to expand their programs significantly, and has approximately 50 new students completing the programs each year. Their success is due to the faculty's efforts to work closely with businesses and to their effective marketing. For more information on EdCC, please visit:

<http://infosec.edcc.edu/>

Other Training Providers

Many private training and education providers such as DeVry University, ITT Technical Institute, Westwood College, the United Education Institute, Versitas, or Hands On Technology Transfer, Inc., offer courses in computer technology. However, the cost of

⁶ <http://rissc.mtsac.edu/>

attending any of these providers' courses is much higher than community colleges' cost. In addition, it is preferable for students to take courses which can be transferred to four-year universities. Obtaining a more advanced degree will expand students' career opportunities in cybersecurity.

Implications and Recommendations for Community Colleges

Opportunity: There is an opportunity for the community colleges to teach courses related to cybersecurity to adequately prepare students for high-growth, high-demand, high-wage occupations, and to keep cybersecurity professionals' skills up-to-date — a continuing effort in this fast-changing field. Computer Information Systems (CIS) programs should include one or more courses on data and network security. Colleges also have the opportunity to offer short-term certificates for incumbent workers (many of whom already have degrees) to keep their skills up-to-date.

Job market: According to AACCC⁷, many jobs such as Network Administrator, Security Administrator or Technician can be filled with employees holding an Associate Degree in cybersecurity. Moreover, a two-year degree can lead to a transfer into a four-year program, and can also be a strong prerequisite to industry-endorsed certifications. Both alternatives make employees extremely valuable in high-demand, high-paying jobs. However, career advancement requires a four-year degree; therefore, colleges must align their courses with university programs to facilitate student transfer.

Partnering with businesses: It is crucial for community colleges to work closely with their local businesses. Offerings may range from Associate Degrees to industry certifications or special courses to teach cybersecurity knowledge and skills, based on employers' specific needs. In addition, business partners may donate equipment, staff time for teaching or participating in advisory committees, and/or offer work-experience opportunities for students. EdCC strongly recommended that colleges partner with local law enforcement and businesses to allow students to work on actual cases. This will (1) attract students wishing to gain work experience, (2) help students find jobs after completion, and (3) strengthen the programs' content and the relationships with employers.

Promoting IT careers: Colleges often report decreasing enrollment in computer and information systems (CIS) programs because the public has an incorrect perception that computer-related jobs are no longer in high-demand. Therefore, colleges may consider working with counselors and high-schools to develop an awareness of the career opportunities. For the programs to succeed, it is very important to develop effective marketing strategies to adequately portray the career opportunities in cybersecurity and attract students into this field. EdCC's most effective marketing activity is to offer free seminars in computer forensics, which brings significant visibility to their information security programs. For more information on the seminars, visit: <http://infosec.edcc.edu/computerforensicsfundamentals.htm>

⁷ Protecting Information: The Role of Community Colleges in Cybersecurity Education. American Association of Community Colleges. June 2002.

Conclusion

Employers reported having difficulty recruiting qualified employees in Los Angeles County, where seven community colleges already offer programs in cybersecurity. The results of the study did not confirm that colleges need to create more programs. However, it became apparent that strong relationships between colleges and businesses were critical to program success. Collaboration is needed to keep the programs current, offer real work experience to students, and help students find employment after completion of the programs.

The need for information technology employees with cybersecurity expertise is expected to continue to grow rapidly. For this reason, colleges offering CIS programs should consider adding classes on data and network security if they do not already do so. This represents an opportunity for community colleges to offer programs leading to high-demand, high-growth, and high-paying jobs in Los Angeles County. However, the faculty teaching cybersecurity must be able to work more closely with employers than they normally do for other programs. Faculty members also need continual training to keep up to date with the latest innovations in the area of security.

Numerous resources such as model programs, curricula and best practices are available to help colleges in their effort to respond quickly and effectively. In addition, grant dollars are available to help colleges offer training in this field. For example, the National Science Foundation (NSF) funded the Regional Information Systems Security Center and encourages colleges and universities to further expand their cybersecurity offerings. For more information, call the Center of Excellence at (909) 594-5611 ext. 6106.

References and Resources

American Association of Community Colleges. The Role of Community Colleges in Cybersecurity Education Report, 2002 . (www.aacc.nche.edu)

Campbell, Robert D. (Rock Valley College) and Hawthorne, Elizabeth K. (Union County College). Cybersecurity Education in Community Colleges Across America: A Survey of Four Approaches by Five Institutions Report, 2002.

Edmunds Community College Digital Forensics and Information Security.
(<http://infosec.edcc.edu/>)

Educators' Website for Information Technology (EWIT).
(<http://tdlcluster.ioes.org/visitoutside.cfm?address=http://www.edc.org/EWIT>)

EDUCAUSE Connect. (www.educause.edu/cybersecurity)

Employment Development Department Labor Market Information.
(www.labormarketinfo.edd.ca.gov/)

Godbe Research. Computer and Information Security Labor Market Study, June 2006.

Higher Education Information Technology Alliance (HEITA). (www.heitalliance.org/)

Internet 2, Networking Consortium. (www.internet2.edu/)

Mt. San Antonio Community College Regional Information Systems Security Center.
(http://rissc.mtsac.edu/RISSC_NEW/default.asp)

National Strategy to Secure Cyberspace. (www.whitehouse.gov/pcipb/)

Power, Richard. "2002 CSI/FBI Computer Crime and Security Survey." *Computer Security Issues and Trends*, vol. 8, no. 1 (Spring 2002). (www.gocsi.com)

APPENDIX A: How to Utilize this Report

About Us - Description of BWPI

The Business and Workforce Performance Improvement (BWPI) initiative is focused on building the capacity of the colleges in the area of economic and workforce development to enhance their ability to deliver education and training services to businesses and workers in high growth industries, new technologies, and other clusters of opportunities.

The Centers of Excellence (COE) within BWPI provide information regarding workforce trends, increasing awareness and visibility about the colleges economic and workforce development programs and services, and building partnerships with business and industry. The difference this will make to the colleges is that it will position them as THE workforce partners of choice to business and industry and ensure that college programs are current and responsive. This will contribute to the overall economic vitality of the communities in which they serve.

How to Use This Environmental Scan Report

The Centers of Excellence within the Business and Workforce Performance Improvement Initiative of the California Community College Economic and Workforce Development Program have undertaken Environmental Scanning to provide targeted and valuable information to community colleges on high growth industries and occupations.

This report is intended to assist the decision-making process of California community college administrators and planners in addressing local and regional workforce needs and emerging job opportunities in the workplace as they relate to college programs. The information contained in this report can be used to guide program offerings, strengthen grant applications, and support other economic and workforce development efforts.

This report is designed to provide current industry data that will:

- Define potential strategic opportunities relative to an industry's emerging trends and workforce needs;
- Influence and inform local college program planning and resource development; and
- Promote a future-oriented and market responsive way of thinking among stakeholders.

This Environmental Scan included a review of the California Regional Economies Project reports and Employment Development Department (EDD) Labor Market Information (LMID) projections that cover the communities in this region, as well as many other sources as referenced.

Important Disclaimer:

All representations included in this report/study have been produced from a secondary review of publicly and/or privately available data and/or research reports. Efforts have been made to qualify and validate the accuracy of the data and the reported findings. The purpose of the Environmental Scan is to assist the California Community Colleges to respond to emerging market needs for workforce performance improvement. However, neither the BWPI Centers of Excellence, COE host college or California Community Colleges Chancellor's Office are responsible for applications or decisions made by recipient community colleges or their representatives based upon this study including components or recommendation.