

May

2004

GRANT APPLICATION

Clover Park Technical College/Edmonds Community College

**Cyber Security Training
and Technical
Assistance**

OFFICE OF COLLEGE RELATIONS

Grants Development

Brandon Rogers
Clover Park Technical College
Grants Development Office
4500 Steilacoom Blvd. SW
Lakewood, WA 98499-4098
Phone 253.589.5501 • eMail brandon.rogers@cptc.edu

Table of Contents

Proposal Abstract	2
Electronic Preparedness and Response Education (E-PARE)	
Abstract.....	2
Narrative.....	5
Project Background and Overview	5
Identification of Problem.....	7
Goals and Objectives	9
System-wide Impact.....	13
Performance Measures/Timelines	16
Budget	20
Budget.....	20



Clover Park provides education leading to competencies that meet business and industry standards for the diverse workforce of today and tomorrow.

Edmonds Community College is a leader in providing quality opportunities for learning and service, responding to the dynamic needs of our diverse community.

Proposal Abstract

Electronic Preparedness and Response Education (E-PARE) Abstract
As set forth in the Office for Domestic Preparedness (ODP) requirements, we have identified the following as our primary issue area:

“Initiatives related to the prevention of cyber terrorism and increased awareness of cyber security issues.”

Clover Park Technical College and Edmonds Community College propose a national training and technical assistance program, responsive to first responders and industry in providing on-site and on-line training in emergency preparedness and response to cyber terrorism. Our goals are threefold:

Curriculum Development: To create a nationally replicable training module focused on combating cyber crime, from assisting law enforcement in investigation/response to helping small businesses maintain operations during electronic attacks.

Training/Outreach: To convene a group of professionals in anti-cyber terrorism who will provide train-the-trainer services and resources to law enforcement and small business.

Clearinghouse Services: To house a library of information and to tap into the already existing network of information, such as US-CERT, encouraging the community college network, small businesses and first responders to report cyber criminal activity.

Building on Edmonds Community College's nationally recognized work in Computer Forensics and Clover Park's National Security Administration (NSA) certified efforts in Computer Information Systems Security, including Business Continuity, the E-PARE project will quickly build a model of national significance in response to cyber terrorism.

Based in the Puget Sound, E-PARE will partner with a statewide Center of Excellence in Homeland Security based at Pierce College, the Homeland Security Institute at the Washington State Patrol, and Ready*Corps, a federally funded volunteer effort in homeland security.

“The Internet now connects over 171,000,000 computers...”

“In the 2003 CSI/FBI Computer Crime and Security Survey, it was reported that computer viruses led to over \$27 million in losses...”

“Total damages from the Blaster worm are estimated to be at least \$525 million.”

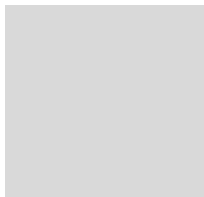
Excerpts from testimony to the Subcommittee on Telecommunications and the Internet, November 6, 2003.

Find more resources at:

www.epare.org



Narrative



Project Background and Overview

(Insert Template from Pierce here?)

The partnership between Clover Park Technical College and Edmonds Community College requests funding from the Office for Domestic Preparedness to implement E-PARE, Electronic Preparedness and Response Education, a national training and technical assistance program for first responders and commerce:

1. E-PARE will bring together faculty and first responders with expertise in computer forensics and business continuity/organizational security to fill in gaps among current cyber preparedness offerings. This curriculum development team will adapt the National Security Administration (NSA) certified curriculum at Clover Park Technical College, combining it with the nationally-recognized computer forensics program at Edmonds Community College to create a training module for police and small business.
2. Upon development of the E-PARE training module, the curriculum development team will identify and recruit a national pool of trainers from the first responder and computer security industry, bringing them together for a certificated train-the-trainer event.

3. Upon receiving this Cyber Crime Certification, which will include articulation agreements for college credit, this national pool of trainers will be qualified to provide prevention awareness training and emergency response to local law enforcement and small business in the area of cyber terrorism. By tapping into the larger network of community colleges, Community Emergency Response Teams (CERTs), State Centers for Excellence in Homeland Security and chambers of commerce, this pool of cyber security responders will serve as a national resource.
4. In addition to providing on-site assistance, E-PARE will develop cyber security kits available to the public. These kits will be the electronic equivalent of first-aid kits, employing a variety of media (video, cd-rom, pamphlets, web resources, etc.), and available to the public.
5. A major component of E-PARE will consist of public awareness and outreach. Unfortunately, the vast majority of computer damages and losses are aided by an unwitting public, unaware that there are resources available to stem this growing area of crime. E-PARE will assist the current US-CERT effort to track and report cyber criminal incidents, and strongly advocate that computer safety becomes just as familiar to the human resources lexicon as are other important issues such as office safety, ergonomics, sexual harassment and equal rights training.
6. Employing a blended approach both to program evaluation and development, E-PARE will use the ADDIE (Analysis, Design, Development, Implementation and Evaluation) method to ensure program quality and effectiveness throughout the 2-year implementation phase funded by ODP.

...the vast majority of computer damages and losses are aided by an unwitting public...

Identification of Problem

In what area(s) can ODP grant funds be used to maximum benefit in the area of cyber-security/cyber-terrorism? (0-20 points)

First and foremost, as is clearly defined in the Homeland Security Presidential Directive 8 and the Homeland Security Act, this Competitive Training Grants Program has identified the first responder community as its primary audience. Specifically, the E-PARE project has targeted law enforcement as having a critical need for cyber-terrorism and computer forensics training.

Last year speaking before the House Appropriations Committee, FBI Director Robert Mueller listed cyber crime as one of the agency's top three priorities, requesting \$234 million to defend against cyber-based attacks and high-technology crimes. Citing figures that show 6 of every 10 investigations require computer forensics support, Mueller stated, "Terrorist groups are increasingly computer savvy, and with publicly available hacker tools, many have the capability to launch nuisance attacks against Internet-connected systems. As terrorists become more computer savvy, their attack options will increase."

While programs of instruction for information security and forensic computing are popping up in community colleges throughout the nation, the majority of faculty lack the knowledge and industry experience needed to fully prepare students for jobs within the disciplines. Before Edmonds Community College developed its Computer Forensics certification, there were no programs within the state of Washington that actively involved law enforcement personnel in the curriculum development or delivery phase of training involving information security. It is important that law enforcement be involved in the overall program design because it's a key employer of qualified individuals in this field. Community colleges are critical to this effort given ***that over 80% of all first responders receive their training through the two-year system of higher education.***

Secondly, true to the spirit of the ODP request for training grant proposals, the partners of E-PARE do not intend to duplicate existing efforts in cyber terrorism defense and cyber security awareness. In reviewing the services offered by current organizations such as US-CERT (the partnership between the Department of Homeland Security and Carnegie Mellon University's CERT Coordination Center), the Forum of Incident Response and Security Teams (FIRST), and the Computer Security Institute, we made a concerted effort to identify areas where we might *augment* overall national preparedness.

Specifically, while larger corporations might have the financial ability and internal infrastructure to deal with electronic threats, small businesses, which employ over half of our nation's workforce and generate more than half of the national gross domestic product, often neglect even very basic cyber protection available, owing to fears of cost, complication and capacity. We recognize that much of current cyber criminal activity takes advantage of an uninformed, but internet-connected, public, and our secondary aim will be to raise this level of awareness.

Unfortunately, a certain level of misinformation seems to permeate public discussion in the area of cyber crime, adding a hint of hysteria to the actual threat. Reminiscent of the Y2K phenomenon, news stories are replete with terms such as "Digital Armageddon," "Electronic Pearl Harbor," and "Electronic Chernobyl." While these terms are meant to evoke the potential seriousness of being caught unprepared, the result in too many instances has been a 'boy-who-cried-wolf' effect, allowing computer users to fall into a false sense of security. By offering a certified-training, this project will lend legitimacy to alerts of potential electronic threats, aiding nation-wide terrorism prevention efforts.

In short, there are two primary problems that this project will address: lack of involvement/training for law enforcement first responders and lack of awareness about how to respond to cyber security threats among the majority of our nation's employers.

Goals and Objectives

How will we accomplish our goals and objectives? (0-25 points)

1. Goal 1- Develop a certified training curriculum involving first-responders and experts within cyber security.

Evidence and Objectives

-
- a. We are qualified to lead a curriculum design team in this field and will successfully accomplish this for several reasons. Clover Park's Computer and Information Systems Security (CISS) program has been recognized by the National Security Agency (NSA) as certified for cyber-security skills education. In fact, Clover Park Technical College is the only two-year college in the Western US to be so recognized.
- b. Edmonds Community College's contributions toward closing the information technology employment gap are equally well known, and they have become a pioneer in the field of computer forensics. According to Community College Week, Edmonds Community College is the fifth highest producer of graduates in information technology of all community colleges in the nation. Edmonds Community College's Computer Forensics program is certified by the CyberSecurity Institute (CSI).

2. Goal 2- Create a cyber terrorism safety kit and access to distance learning that will benefit small businesses, non-profit organizations and educational institutions.

Evidence and Objectives

-
- a. Both Edmonds Community College and Clover Park Technical College house state of the art resources for business and education. Clover Park Technical College is home to the Rainier Media Center, which will allow for the inclusion of multimedia materials (video, cd-rom, dvd) in the cyber terrorism safety kit.

- b. The Small Business Development Center at Edmonds Community College is a local leader in developing resources for business, which from 1999-2002 helped business owners obtain a record level of over \$5 million in financing.
- c. Both institutions are experienced distance learning providers. Both training and electronic versions of the cyber terrorism safety kit will be available via the internet, following the FEMA model in CERT training delivery.

3. Goal 3- Establish a national team of experts available nationwide in times of cyber terrorist attacks.

Evidence and Objectives

-
- a. Recently asked to lead the ODP funding application process for Cyber Security by the Washington State Board of Community and Technical Colleges, the Clover Park/Edmonds partnership is directly connected to the larger network of homeland security agencies which represent the US military, law enforcement, fire departments and government.
 - b. Our affiliation with the Washington Center of Excellence in Homeland Security is part of a national effort which connects us to virtually every community college in the nation through the American Association of Community Colleges. This network, which we believe distinguishes our proposal for training, is important because the 1,173 two-year colleges in this country train over 80% of all first responders and educate over 10 million students each year. These partnerships will ensure our ability to field a well-qualified team of trainers.

4. Goal 4- Raise public awareness regarding the importance of cyber security.**Evidence and Objectives**

-
- a. Using a train-the-trainer approach, our curriculum will consist of three tracks, one of which will focus on public awareness and outreach (the other two, as mentioned above, are targeted specifically to 1) law enforcement in the area of computer forensics and 2) small businesses in the area of business continuity and organizational security.
 - b. Partnering with Ready*Corps, a homeland security initiative funded by the Corporation for National and Community Service, we will reach out to the national network of Citizen Corps Councils, who act as local repositories of emergency resource information.
 - c. After the development and piloting stage of E-PARE, we will launch a public relations campaign as well as travel to regional conferences to present our accomplishments and findings.

5. Goal 5- Serve as a cyber security resource clearinghouse as part of our respective computer information security mandates.**Evidence and Objectives**

-
- a. As we are already committed to teaching cyber security to business and industry in Washington State, ODP funds will be used to supplement our existing plans for providing cyber security resources to the public.
 - b. We will establish a lending library of hard-copy resources, available to first responders, who can request those materials through the mail.

- c. We will link through our web site, www.epare.org, to the wide array of currently existing databases of information, and organize these in a way which is easy to understand.

6. Ancillary Goals-

- a. Strengthen current degree and certificate offerings in Computer Information Systems Security and Computer Forensics, using our efforts through E-PARE to serve as a model to other academic programs nationwide.
- b. Boosting recruitment of students nationwide to become computer security professionals by bringing to public awareness the importance of this field to homeland security efforts.



System-wide Impact

What are the project's strategies for reaching a significant number of public safety personnel through a cross-disciplinary approach? Describe current partnerships. (0-25 points)

Strategy 1- Build on Existing Partnerships in Homeland Security.

Because we have been asked to lead this ODP grant application effort for Washington State by the Washington State Board of Community and Technical Colleges, we have an established partnership with many of the key players in homeland security, including 1) the Homeland Security Institute, to be housed at the Washington State Patrol, 2) the Washington Emergency Management Department, which oversees state-wide emergency management at Camp Murray and 3) the US military, through Fort Lewis and McChord Air Force Base, both within 15 minutes of our campus.

The American Association of Community Colleges (AACC) has already partnered with our State Board to draft proposals in each of the areas of concern to ODP. This uniquely places the E-PARE project in connection with a national network of 1,173 community colleges, which train over 80% of the nation's first responders.

Clover Park Technical College and Edmonds Community College have long-standing ties to first responders due to our various degree and certificate programs, which also include Fire Administration, Allied Health Education, Emergency Management, Aviation Maintenance, Environmental Mitigation/HAZMAT, Practical Nursing and Emergency Communication.

In addition, we also received staffing commitment from Ready*Corps, a program funded by the Corporation for National and Community Service focusing on disaster response, with members in all 50 states.

Strategy 2- Build on Existing Partnerships in Computer Security among Academia and Business Professionals.

While first responders are critical to national efforts in homeland security, we also believe that academia and business have vital, and often overlooked, roles to play.

As the only two-year college in the Western US to be recognized by the National Security Agency (NSA) as certified for cyber-security skills education, we are automatically linked to all the four-year universities designated by the NSA as Centers of Academic Excellence in Information Assurance. We can recruit appropriate faculty through this network to strengthen our training design.

Among our business/industry connections includes the CEO of CyberSecurity Institute, who in addition to teaching at Edmonds Community College also trains businesses in computer security.

Strategy 3- Take Full Advantage of our Instructional and Outreach Capabilities.

As institutions of higher education, we are experts in cross-disciplinary instruction. Representing community and technical colleges, we are also keenly aware of the importance of applying adult learning theory to our curricula. Both of our institutional missions demand that we be responsible to the changing needs of business and industry, and as such, we have the following advantages:

- distance learning technology/experience
- advanced audio-video capabilities, including a television/radio station
- a state-of-the art small business development center
- faculty with established success in educating computer security professionals

Strategy 4- Create Mechanisms for Long-Term Project Sustainability.

We realize that reaching a significant number of public safety personnel is a marathon and not a sprint. Our belief is that any project funded through ODP should have a plan for ensuring that the training does not end after the two-year funding cycle.

Our advantage in this category is that we are not designing a program from scratch, but adapting from current curriculum that has already proven successful. As our past experience will strengthen the E-PARE project, so will the E-PARE findings inform our academic offerings.

Furthermore, by providing our findings regarding the importance of computer forensics training for police officers, long-term sustainability among these first responders will be strengthened as police departments begin to reserve larger portions of their budget to an issue critical to both local and national homeland defense.

By enlisting Ready*Corps, we have already tied into a federal program whose mission is dedicated to sustainability and capacity-building. Ready*Corps staff will educate and inform the national network of Citizen Corps councils, who will serve as lasting resources for local communities. Ready*Corps has made a 3-year commitment to our program.

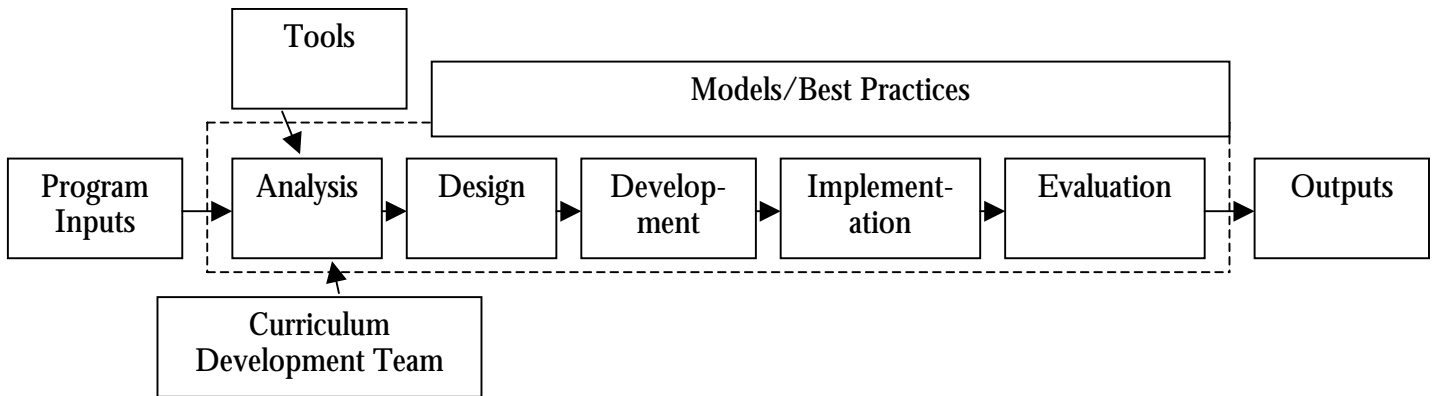
Finally, by publicizing the effectiveness of our business continuity model, we will educate small business owners about the benefits of pooling resources when they feel they cannot individually afford technical support, as well as the downfalls of ignoring this threat. In this manner, E-PARE will help share ODP's message of preparedness with a larger public. Long term, we feel that our 'Computer Security Video' will be as sought after by human resources offices nationwide as are videos in sexual harassment training, ergonomics, office safety, etc.

Performance Measures/Timelines
How will program effectiveness be measured at regular intervals throughout the project period? (0-10 points)

In order to determine our effectiveness, as well as remain compatible with ODP standard procedures, we have adopted the ADDIE (Figure 1) method in creating our timeline, our outcomes and our performance measurements.

We will measure our key benchmarks at quarterly intervals.

Figure 1. ADDIE Adaptation for E-PARE Project



• **Year One, First Quarter: Inputs, Analysis**

- In the first 3 months of E-PARE, our core curriculum development team, including lead faculty at each college, will collect best practices and begin design modification of computer forensics and business continuity course work (tools).
- Staffing for the coordination of the overall project will be hired during the first quarter of the E-PARE project.
- Ready*Corps staff will begin outreach to local homeland security agencies and collect resources for eventual Cyber Security Clearinghouse.

Benchmarks:

1. *Initial design process approved for Computer Forensics Short-Course Curriculum Adaptation according to CyberSecurity Institute standards.*
2. *Clearinghouse model established.*

3. *Pre-test Instrument Developed by Institutional Research*

• **Year One, Second Quarter: Analysis (cont.), Design**

- Curriculum development team will spend the bulk of the second quarter writing the final curricula for computer forensics and business continuity training.
- Project staff will coordinate TOT logistics, including adapting writing to create written materials, locating a conference site, facilitating the selection of the national training team.
- Public Relations/outreach to homeland security agencies begins in earnest; epare.org web site launch.

Benchmarks:

1. *Identification of 60 national/regional specialists to serve as initial training team.*
 2. *Memoranda of cooperation signed with at least three other national homeland security organizations for coordination of efforts.*
 3. *Pre-test of needs administered to key stakeholders.*
-

• **Year One, Third Quarter: Development Stage**

- Curriculum development team and project staff will iron out instructional roles for TOT delivery.
- Initial cyber security emergency kit (with exception of video, cd-rom) will go to production/publication/duplication.
- Cyber security resource library opens to internal partners for test phase.

Benchmarks:

1. *TOT instructors named.*
 2. *TOT curriculum submitted to partner agencies for final review/comments.*
 3. *Pre-test instrument evaluated by Institutional Research for final inclusion in TOT.*
-

• **Year One, Fourth Quarter: Implementation, Stage One**

- 3-5 day TOT held for cyber security national training team, focusing on two tracks (computer forensics and business continuity) and outreach.
-

- Cyber security emergency kits released to training team.

Benchmarks:

1. *National training team satisfaction with model/curriculum.*
 2. " " " " " *cyber security emergency kit.*
 3. *Initial communities/organizations designated for delivery of training/awareness.*
-

- **Year Two, First Quarter: Implementation, Stage Two**

- First group of TOT recipients apply training to local communities, coordinated by Ready*Corps.
- Second stage of outreach (video production, media releases) implemented.

Benchmarks:

1. *Local recipients satisfied with level and availability of training*
 2. *Agency satisfaction with services offered by resource lending library.*
 3. *Activities covered by media outlets.*
-

- **Year Two, Second Quarter: Measurement/Evaluation**

- Second group of TOT recipients apply training in local communities.
- Core curriculum team meeting to evaluate areas of effectiveness/improvement.

Benchmarks:

1. *Increase of local agency satisfaction with cyber security training*
 2. *Continued increase of requests of lending library resources.*
 3. *Web site, including searchable database of national training team members and locations, completed.*
-

- **Year Two, Third Quarter: Outputs**

- Identification of post-ODP partners, including law enforcement agencies and business organizations.
- Findings reported in appropriate journals, to relevant conferences.

Benchmarks:

1. *Articulation agreements established for college credit.*
-

2. *60 total trainings delivered, cumulatively (at least one per national training team member).*

• **Year Two, Fourth Quarter: Final Analysis**

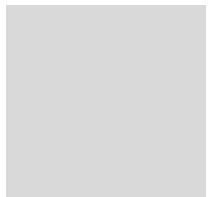
- Continued delivery of local training.
- Final report delivered to ODP.

Benchmarks:

1. *ODP satisfied with program findings/overall effectiveness.*
 2. *Number of local requests for trainers doubles from third quarter.*
-



Budget



Budget
(attached as spreadsheet)