CYBER SECURITY EDUCATION: MEETING THE NEEDS OF TECHNOLOGY WORKERS AND EMPLOYERS

HEARING

BEFORE THE

COMMITTEE ON SCIENCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

—————

JULY 21, 2004

—————

Serial No. 108–68

—————

Printed for the use of the Committee on Science

Available via the World Wide Web: http://www.house.gov/science

—————

COMMITTEE ON SCIENCE

HON. SHERWOOD L. BOEHLERT, New York, *Chairman*

RALPH M. HALL, Texas
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
KEN CALVERT, California
NICK SMITH, Michigan
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
GIL GUTKNECHT, Minnesota
GEORGE R. NETHERCUTT, JR.,
   Washington
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
WAYNE T. GILCHREST, Maryland
W. TODD AKIN, Missouri
TIMOTHY V. JOHNSON, Illinois
MELISSA A. HART, Pennsylvania
J. RANDY FORBES, Virginia
PHIL GINGREY, Georgia
ROB BISHOP, Utah
MICHAEL C. BURGESS, Texas
JO BONNER, Alabama
TOM FEENEY, Florida
RANDY NEUGEBAUER, Texas
VACANCY

BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
NICK LAMPSON, Texas
JOHN B. LARSON, Connecticut
MARK UDALL, Colorado
DAVID WU, Oregon
MICHAEL M. HONDA, California
BRAD MILLER, North Carolina
LINCOLN DAVIS, Tennessee
SHEILA JACKSON LEE, Texas
ZOE LOFGREN, California
BRAD SHERMAN, California
BRIAN BAIRD, Washington
DENNIS MOORE, Kansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
DENNIS A. CARDOZA, California
VACANCY
VACANCY
VACANCY

CONTENTS

July 21, 2004

Appendix: Answers to Post-Hearing Questions

CYBER SECURITY EDUCATION: MEETING THE NEEDS OF TECHNOLOGY WORKERS AND EMPLOYERS

————————

WEDNESDAY, JULY 21, 2004

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE,
Washington, DC.

The Committee met, pursuant to call, at 10 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Sherwood L. Boehlert (Chairman of the Committee) presiding.

COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

Cyber Security Education: Meeting the Needs of Technology Workers and Employers

Wednesday, July 21, 2004
10:00 a.m.-12:00 p.m.
2318 Rayburn House Office Building (WEBCAST)

Witness List

Mr. Chet Hosmer
President & CEO
WetStone Technologies, Inc.

Mr. John Baker
Director, Technology Programs, Division of Undergraduate Education
School of Professional Studies in Business and Education
Johns Hopkins University

Mr. Erich Spengler
Principal Investigator, Advanced Technology Education Regional Center for the Advancement
of Systems Security and Information Assurance
Moraine Valley Community College

Second Lieutenant David Aparicio
Developmental Electrical Engineer, Information Directorate
Air Force Research Laboratory

Ms. Sydney Rogers
Principal Investigator, Advanced Technology Education Regional Center for Information
Technology
Nashville State Community College

3

HEARING CHARTER

COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

Cyber Security Education:
Meeting the Needs of
Technology Workers and Employers

WEDNESDAY, JULY 21, 2004
10:00 A.M.–12:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

1. Purpose

On Wednesday, July 21, 2004, the House Committee on Science will conduct a hearing to review efforts by academia, industry and government to develop a cyber security workforce.

2. Witnesses

Mr. Chet Hosmer is the President & CEO of WetStone Technologies, Inc. of Cortland, New York. Mr. Hosmer has taught Network Security and Cyber-Crime and Computer Forensic courses at Utica College, and he is the Research Advisor for the Computer Forensics Research and Development Center of Utica College. Mr. Hosmer also is Co-chair of the Electronic Crime and Terrorism Partnership Initiative's Technology Working Group at the National Institute of Justice.

Mr. John Baker is the Director of Technology Programs for the Division of Undergraduate Education of the School of Professional Studies in Business and Education at the Johns Hopkins University in Baltimore, Maryland.

Mr. Erich Spengler is the head of the Regional Center for the Advancement of Systems Security and Information Assurance at Moraine Valley Community College in Palos Hills, Illinois.

Second Lieutenant David Aparicio is an electrical engineer for the Air Force Research Laboratory Information Directorate in Rome, New York. Lt. Aparacio is a graduate of the "Cyber Security Boot Camp" run jointly by the Air Force, Syracuse University, the New York State Office of Science, Technology and Academic Research.

Ms. Sydney Rogers is the head of the Regional Center for Information Technology at Nashville State Community College in Nashville, Tennessee. Ms. Rogers is also the Vice President for Community and Economic Development at the community college and her responsibilities include workforce development, computer services and distance education.

3. Overarching Questions

The hearing will address the following overarching questions:

- How are academia, industry and government working together to meet the Nation's cyber security education and training needs?
- What are the strengths and weaknesses of existing cyber security education and training programs?
- What new and emerging challenges need to be addressed in this area? How can the Federal Government contribute to this effort?

4. Brief Overview

- Information technology systems play a critical role in today's economy, yet they are vulnerable to security breaches and attacks. Adequately protecting these systems requires, among other things, a well-trained cyber security workforce to block, detect and counter any threats to vital computer systems and networks.

4

- In 2002, the President signed into law the *Cyber Security Research and Development Act* (P.L. 107–305), which originated in the Science Committee. The Act effectively designated the National Science Foundation (NSF) as the lead agency for civilian cyber security research and education, and it authorized $216 million over FY 2003–FY 2007 for NSF cyber security education and training programs. The Act also authorized advanced cyber security education and training programs at the National Institute of Standards and Technology (NIST), but these programs have never been funded.
- The National Security Agency (NSA) also is engaged in cyber security education and training. In addition, the Department of Homeland Security (DHS) supports public awareness and outreach on cyber security vulnerabilities and countermeasures, and it helps coordinate private-sector efforts with those of the Federal Government.
- As the challenges of cyber security emerge and evolve, so too do the courses and programs of cyber security education and training. From programs in traditional settings, like two- and four-year colleges and universities, to other programs, like the Cyber Security Boot Camp, the cyber security education and training continuum is growing and becoming more standardized in its effort to meet the needs of technology workers and employers.

5. Background

Estimates of annual economic losses caused by computer virus and worm attacks and to hostile digital acts in general run from about $13 billion (worms and viruses only) to $226 billion (for all forms of overt attacks). While the precise figures are open to question, there is no doubt that cyber security intrusions result in significant losses due to downtime, lost productivity, and expenses related to testing, cleaning and deploying patches to computer systems.

Experts increasingly point out that improving cyber security requires cyber security training for technicians and users, in addition to promulgating sound security practices and deploying sophisticated technology. As one security professional explained, you can be "bristling with firewalls and IDS (intrusion detection systems), but if a naïve user ushers an attacker in through the back door, you have wasted your money."

Education and Training Needs

Many system failures and security breaches occur because of human error. Employees may fail to install a patch, or configure a firewall incorrectly, or otherwise leave a system open to intrusion. Such errors occur, in part, because responsibility for security traditionally has fallen to non-security workers who may lack the time, training and focus to handle such responsibilities.

A 2002 report by the National Workforce Center for Emerging Technologies and the Computing Technology Industry Association (CompTIA) found that many security organizations were beginning to seek security professionals, deciding that it was no longer acceptable just to buy a firewall package, install it, and let it run.

Industry is also increasingly interested in fostering concern with cyber security at all the levels of the workforce dealing with computers from administrative workers (such as network administrators, technicians, and help desk staff) to engineers (including software developers) to system architects.

Responding to that interest, cyber security education and training is increasingly being offered through degree-granting programs at both two- and four-year colleges and universities, but also through shorter, credit and non-credit programs that provide certificates or provide background for students to pass certification exams.

Federal Support for Cyber Security Education and Training

National Science Foundation

Federal Cyber Service: Scholarship for Service (SFS)—The program has two aspects—a "Scholarship Track" that provides grants to colleges and universities for student stipends, and a "Capacity-Building Track" that provides grants to colleges and universities to improve their ability to provide courses in cyber security.

The Scholarship Track provides four-year grants to colleges and universities, which, in turn, use the money to provide as many as 30 two-year scholarships. In exchange for two years of stipends ($8,000 per year for undergraduate students and $12,000 for graduate students) and a summer internship at a federal agency, participating students are required to work for two years in the Federal Cyber Service for a federal agency. Since 2001, 391 individuals have participated in the scholarship program.

The Capacity Building Track provides two-year grants of up to $150,000 per year for such activities as adapting and implementing the use of educational materials, courses or curricula; offering technical experience; developing laboratories, and offering faculty development programs. (An additional $150,000 per year is available to partnerships that include minority serving institutions.)

The SFS program was funded at $16.1 million in Fiscal Year (FY) 2004, and the Administration request for FY 2005 is $16.2 million. A list of colleges and universities participating in the SFS program is provided in Appendix II.

Advanced Technology Education (ATE)—ATE is NSF's program to improve technical education at two-year colleges. Grant awards may involve partnerships between two-year and four-year institutions.

One aspect of ATE is the funding of regional centers (such as the two giving testimony at this hearing), which are designed to create model programs in specific areas, such as cyber security, to adapt those programs to local needs, provide professional development for college faculty, and help recruit, retain and place students.

The ATE program, which received $45.23 million in FY 2004, of which about $3.7 million will be invested in cyber security education and training (although the breakdown for cyber security is a very rough estimate).

National Security Agency

The National Security Agency (NSA) established the Centers of Academic Excellence in Information Assurance Education (CAE/IAE) Program in 1998 to increase the number of professionals with information assurance expertise in various disciplines. The CAE/IAE Program endorses qualified four-year and graduate information assurance degree programs (including those at Johns Hopkins, which is testifying at this hearing).[1] Currently, there are 59 universities in 27 states that are designated as CAE/IAE (see list in Appendix III). Being designated a CAE/IAE does not guarantee an institution funding, but it is a "seal of approval" that facilitates applying to grant programs, and it makes institutions eligible for certain NSA programs.[2]

NSA also manages an SFS program in information assurance for the Department of Defense (DOD). This program is similar to the one run by NSF, with scholarships provided for study at a CAE/IAE in return for a student's service at a DOD agency. Currently 82 students are participating in the NSA SFS program.

Department of Homeland Security

The Department of Homeland Security (DHS) is working to increase cyber security awareness, foster cyber security training and education programs, and promote private sector support for well-coordinated, widely recognized professional cyber security certifications. In these areas, DHS plays a supporting role, consulting on the efforts and programs underway in other government agencies, at universities, and in the private sector.

6. Witness Questions

Questions for Mr. Hosmer

- In your experience, what knowledge and skills are currently needed in the cyber security workforce? Have cyber security education and training programs been sufficiently flexible to respond to these needs as well as the needs of traditional and returning students?

- What are the current strengths and weaknesses in cyber security education and training programs? Do model programs exist and, if they do, are they being adapted to meet local cyber security needs?

- What partnerships should two-year and four-year colleges and universities forge with business and industry to build appropriate programs? In your opinion, is there sufficient collaboration with industry at the administration (advisory committees), faculty (return-to-industry) and student (internship) levels to accommodate rapid changes in these professional and technical areas?

- What can the Federal Government do to improve cyber security education and build the Nation's technical workforce?

---

[1] Prospective institutions must meet rigorous standards to receive the national recognition and the CAE/IAE designation, including courseware that is certified under the National Security Telecommunications and Information Systems Security Standards as well as ten other criteria describing dimensions, depth and maturity of the information assurance program.

[2] NSA competitively awards a small amount of funding (a few million dollars) for capacity building—curriculum development, purchase of infrastructure for courses—at CAE/IAE schools.

Questions for Mr. Baker

- What are the various levels of cyber security education and training, e.g., systems administration, systems engineering, and systems architecture? What role does your university play in this education and training continuum? How do two- and four-year colleges and institutions collaborate—if at all—to identify and fill cyber security educational needs?
- What are the current strengths and weaknesses of cyber security education and training programs? What courses and programs currently exist? And what programs need to be developed and more broadly implemented?
- What are the challenges to faculty preparation, recruitment and retention in cyber security? How has your university attempted to address these challenges?
- What can the Federal Government do to improve cyber security education and build the Nation's technical workforce?

Questions for Mr. Spengler

- What role do community colleges play in the training of new workers and the retraining of current workers? What employment opportunities in cyber security are available for individuals with a certificate or a two-year degree?
- What are the current strengths and weaknesses of cyber security education and training programs? What "model" courses and programs currently exist? And what types of courses or programs need to be developed or more broadly implemented?
- What are the challenges do you face in recruiting and training cyber security faculty? What type of programs or opportunities do you provide to help keep faculty current?
- What can the Federal Government do to improve cyber security education and build the Nation's technical workforce?

Questions for Lt. Aparicio

- How did your experience at the ACE change your view of cyber security issues? Is this a good way to recruit engineering and other science and technology students into the field? How did your experience in the course influence your career plans?
- Do you think that the combination of education, problem solving and immersion is an effective model for other education and training programs? Why or why not?
- In your opinion, what can the Federal Government do to improve cyber security education and build the Nation's technical workforce?

Questions for Ms. Rogers

- What role do community colleges play in the training of new workers and the retraining of current workers? What employment opportunities in cyber security are available for individuals with a certificate or a two-year degree?
- What are the current strengths and weaknesses of cyber security education and training programs? What "model" courses and programs currently exist? And what types of courses or programs need to be developed or more broadly implemented?
- What are the challenges do you face in recruiting and training cyber security faculty? What type of programs or opportunities do you provide to help keep faculty current?
- What can the Federal Government do to improve cyber security education and build the Nation's technical workforce?

Appendix I: NSF ATE Award Abstracts

Tennessee Information Technology (TN IT) Exchange Center

Start Date: September 15, 2002

Expires: August 31, 2005 (Estimated)

Expected Total Amount: $1,798,803 (Estimated)

Investigator: Sydney U. Rogers sydney.rogers@nscc.edu (Principal Investigator current))

Sponsor: Nashville St Tech Community College, 120 White Bridge Rd., Nashville, TN 37209–4515; 615/353–-3236

The Tennessee Information Technology (IT) Exchange Center provides an effective workforce capacity building system by increasing the IT educational strength in a consortium of two year colleges, four year colleges, secondary schools and industries in North Central Tennessee. The goal is to develop a sustainable Center to meet the needs of industry for a qualified IT workforce by creating real world scenarios based on industrial needs and using them as the basis for instruction in IT courses. The learning strategies are developed in workshops at the Center for Learning and Teaching at Vanderbilt University. The cases are used in high school academies to interest high school students in IT careers. A web site provides information about the availability and content of education and training programs in the region, a clearinghouse of job opportunities and regular communications among partners. Regional stakeholder forums bring industry and educators together to develop a shared vision based upon research for effective delivery of instruction. The audience includes both students in educational institutions and re-careering workers.

Center for the Advancement of Systems Security and Information Assurance (CASSIA)

Start Date: September 1, 2003

Expires: August 31, 2007 (Estimated)

Expected Total Amount: $2,997,615 (Estimated)

Investigator: Erich Spengler spengler@morainevalley.edu (Principal Investigator current)

Sponsor: Moraine Valley Community College, 10900 South 88th Avenue, Palos Hills, IL 60465–2175; 708/974–4300

This regional center for information technology (IT) security and data assurance serves a five-state area of the Midwest and focuses on a field which is critical to homeland security and which has a large demand for qualified workers. The center builds on a previous Advanced Technological Education project at Moraine Valley Community College, "Applied Internet Technology: Curriculum and Careers" (NSF Award No. 9950037; see http://www.fastlane.nsf.gov/servlet/ showaward?award=9950037 and http://www.morainevalley.edu/nsf/), which concluded in 2002. The following educational institutions are collaborating in the operation of the center: Moraine Valley Community College, Rock Valley College, University of Illinois at Springfield, Lakeland Community College, Washtenaw Community College, Inver Hills Community College, and Madison Area Technical College. Other organizations from business, industry, and government are also advising the center and participating in its activities.

The center is collecting, adapting, and enhancing curricula in cyber security, offering certificate and degree programs, and providing professional development for college faculty in the region. In particular, the center is establishing an A.A.S. degree and a certificate in IT security and data assurance; a concentration in IT security and data assurance within a B.S. degree program in computer science; an Internet-accessible laboratory environment that demonstrates and simulates security technologies; "train the trainer" summer workshops and externship opportunities for faculty from regional community colleges and four-year institutions; an internship program for students in the A.A.S. and B.S. degree programs; and a comprehensive out-

reach and support program to increase the number of students from under-represented groups who pursue IT careers.

Appendix II. Institutions Involved in NSF's Cyber Security Scholarships for Service Program

Institutions with Students in NSF's Cyber Security Scholarships for Service Program[3]

Carnegie Mellon University
Clark Atlanta University
Florida State University
George Washington University
Georgia Institute of Technology
Idaho State University
Iowa State University
Jackson State University
Johns Hopkins University
Morehouse College
Mississippi State University
Naval Postgraduate School
New Mexico Institute of Mining & Technology
Norwich University
Polytechnic University
Purdue University
Spelman College
SUNY at Stony Brook
Syracuse University
University of Idaho
University of Nebraska at Omaha
University of North Carolina at Charlotte
North Carolina A&T University
University of Tulsa

Institutions Receiving Capacity Building Grants via NSF's Cyber Security Scholarships for Service Program

Adelphi University
Amherst College
California State at Long Beach
Carnegie Mellon University
Clark Atlanta University
CUNY Brooklyn
CUNY Borough of Manhattan Community College
CUNY NYC College of Technology
Embry Riddle Aeronautical University
Florida Agricultural and Mechanical University
Florida State University
George Washington University
Georgia Institute of Technology
Hampshire College
Indiana University of Pennsylvania
Illinois Institute of Technology
Indiana University
Iowa State University
Jackson State University
John Jay College of Criminal Justice
Kentucky State University

---

[3] NSF does not directly fund students in the Scholarships for Service program. Instead, funding is provided to institutions who select the scholarship recipients.

Mississippi State University
Mount Holyoke College
Murray State University
Naval Postgraduate School
New Mexico Institute of Mining and Technology
North Carolina Agricultural and Technical State University
North Dakota State University at Fargo
Pennsylvania State University
Polytechnic University
Purdue University
Smith College
Stevens Institute of Technology
SUNY Albany
SUNY at Stony Brook
Texas A&M
University of Alaska-Fairbanks
University of Denver
University of Houston
University of Idaho
University of Kansas
University of Louisville Research Foundation
University of Massachusetts at Amherst
University of Missouri
University of North Carolina at Charlotte
University of Pittsburgh
University of Rhode Island
University of Southern California
University of South Carolina at Columbia
University of Washington
University of Wisconsin-Stevens Point
University of Wisconsin-Parkside
University of Wisconsin-Milwaukee
Towson University
Utica College
Wichita State University

Appendix III: NSA Centers of Academic Excellence in Information Assurance Education

Alabama

Auburn University

California

Naval Postgraduate School
Stanford University
University of California at Davis

Florida

Florida State University

Georgia

Georgia Institute of Technology
Kennesaw State University

Idaho

Idaho State University
University of Idaho

Illinois

University of Illinois at Urbana-Champaign

Indiana

Purdue University

Iowa

Iowa State University

Maryland

Capitol College
Johns Hopkins University
Towson University
University of Maryland, Baltimore County
University of Maryland University College

Massachusetts

Boston University
Northeastern University
University of Massachusetts, Amherst

Michigan

University of Detroit, Mercy
Walsh College

Mississippi

Mississippi State University

Nebraska

University of Nebraska at Omaha

New Jersey

New Jersey Institute of Technology
Stevens Institute of Technology

New Mexico

New Mexico Tech

New York

Pace University
Polytechnic
State University of New York, Buffalo

State University of New York, Stony Brook
Syracuse University
U.S. Military Academy, West Point

North Carolina

North Carolina State University
University of North Carolina, Charlotte

Ohio

Air Force Institute of Technology

Oklahoma

University of Tulsa

Oregon

Portland State University

Pennsylvania

Carnegie Mellon University
Drexel University
East Stroudsburg University
Indiana University of Pennsylvania
Pennsylvania State University
University of Pennsylvania
University of Pittsburgh
West Chester University of Pennsylvania

South Dakota

Dakota State University

Texas

Texas A&M University
University of Dallas
University of North Texas
University of Texas, Dallas
University of Texas, San Antonio

Vermont

Norwich University

Virginia

George Mason University
James Madison University
University of Virginia

Washington

University of Washington

Washington, D.C.

George Washington University
Information Resources Management College

13

Chairman BOEHLERT. The hearing will come to order. Let me explain to our witnesses that both parties had morning conferences, party conferences, and they were running a little bit later than expected, so the Committee is more important than the party, and that is why Mr. Gordon and I are here to welcome you.

It is a pleasure to welcome everyone here this morning for a hearing on cyber security, a subject that has consumed the Committee over the past couple of years. We have focused on this topic for good reason. Information and communication systems underpin our government, and they ensure the smooth functioning of our industries, financial institutions, and transportation systems. They touch nearly every aspect of our lives, but they are fragile, vulnerable to intrusions and attacks.

We continue to focus on new tools to prevent devastating attacks, and we will undoubtedly revisit the federal investment in cyber security research and development in the future, the very near future. But today, we will focus on another cyber security challenge, the education and training of a cadre of professionals in computer security and information assurance.

As the cost of security breaches rise and attacks increase in frequency and sophistication, business and industry are recognizing the need to invest in technology as well as training. And education and training programs are springing up to meet that need. Some of these programs, including those that will be discussed here today, are particularly innovative. But the field of cyber security education and training is still developing. You might say it is in its infancy, and we need to see that it goes to full maturity. We need to learn how to help our colleges and universities respond rapidly and intelligently to a field that continues to evolve. We need to identify ways to attract and retain skilled faculty, and we need to work with higher education institutions, businesses, and other organizations to ensure that education and training courses and programs translate into employment.

If I might give a parenthetical thought for a minute, I am a senior Member on the House Committee on Intelligence, and we are on the eve of the report of the 9/11 Commission. And that report will emphasize something that we are going to emphasize here today: the importance of the investment in human capital.

A few years ago, a friend summed up the challenges of cyber security in this way: "New technologies and enhanced security practices are like sun screen: they offer you some protection, but sooner or later, you are going to get burned." By increasing the quality and quantity of cyber security education and training programs, a new generation of technicians and technology professionals can enhance the SPF of our information and communication systems and create a more secure future. And that would provide a very sunny outlook, indeed.

Chairman BOEHLERT. With that, let me recognize the distinguished gentleman from Tennessee, the Ranking Member, Mr. Gordon.

[The prepared statement of Chairman Boehlert follows:]

14

It is a pleasure to welcome everyone here this morning for a hearing on cyber security—a subject that has consumed the Committee over the past couple of years.

We have focused on this topic for good reason. Information and communication systems underpin our government and they ensure the smooth functioning of our industries, financial institutions and transportation systems. They touch nearly every aspect of our lives, but they are fragile, vulnerable to intrusions and attacks.

We continue to focus on new tools to prevent devastating attacks—and we will undoubtedly revisit the federal investment in cyber security research and development in the future—but today we will focus on another cyber security challenge: the education and training of a cadre of professionals in computer security and information assurance.

As the costs of security breaches rise and attacks increase in frequency and sophistication, business and industry are recognizing the need to invest in technology as well as training. And education and training programs are springing up to meet that need.

Some of these programs, including those represented here today, are particularly innovative, but the field of cyber security education and training is still developing. We need to learn how to help our colleges and universities respond rapidly and intelligently to a field that continues to evolve. We need to identify ways to attract and retain a skilled faculty. And we need to work with higher education institutions, businesses and other organizations to ensure that education and training courses and programs translate into employment.

A few years ago, a friend summed up the challenges of cyber security in this way: New technologies and enhanced security practices are like sun screen. They offer you some protection but, sooner or later, you are going to get burned. By increasing the quality and quantity of cyber security education and training programs, a new generation of technicians and technology professionals can enhance the SPF of our information and communication systems and create more secure future.

And that would provide a very sunny outlook indeed.

Mr. Gordon.

Mr. GORDON. Thank you, Mr. Chairman.

I am pleased to join you in welcoming our witnesses to this hearing on efforts to improve education and training of cyber security professionals. The President's strategy for security in cyberspace highlighted that a lack of trained personnel and inadequate certification programs for security professionals is complicating the task of reducing the vulnerabilities of the Nation's network information systems. This committee also recognized the problem and attempted to address it in the Cyber Security R&D Act, which was enacted during the last Congress.

In addition to new research programs at NSF and NIST, it authorized educational programs at NSF to improve cyber security education at undergraduate institutions, including two-year colleges. These are the education programs that produce the computer and network specialists who are responsible for ensuring that cyber systems are operating safely and reliably.

Today, the Committee will get a progress report on these NSF programs from those in the field who are carrying them out. We also hope to gain a better understanding of the overall state of cyber security education and training. I am interested in whether the federally-sponsored education and training programs are focused on industry's requirements, are meeting the demand that exists for cyber security professionals, and receiving funding that is adequate to ensure that the programs are effective and of sufficient size to meet the need.

Again, I want to welcome the witnesses today and look forward to our discussion.

[The prepared statement of Mr. Gordon follows:]

PREPARED STATEMENT OF REPRESENTATIVE BART GORDON

Mr. Chairman, I am pleased to join you in welcoming our witnesses to this hearing on efforts to improve the education and training of cyber security professionals.

The President's Strategy to Secure Cyberspace highlighted that a lack of trained personnel and inadequate certification programs for security professionals is complicating the task of reducing the vulnerabilities of the Nation's networked information systems.

This committee also recognized the problem and attempted to address it in the Cyber Security R&D Act, which was enacted during the last Congress.

In addition to new research programs at NSF and NIST, the Act authorized education programs at NSF to improve cyber security education at undergraduate institutions, including two-year colleges. These are the education programs that produce the computer and network specialists who are responsible for ensuring that cyber systems are operated safely and reliably.

Today the Committee will get a progress report on these NSF programs from those in the field who are carrying them out. We also hope to gain a better understanding of the overall state of cyber security education and training.

I am interested in whether the federally sponsored education and training programs are focused on industry's requirements, are meeting the demand that exists for cyber security professionals, and are receiving funding that is adequate to ensure the programs are effective and of sufficient size to meet the need.

Again, I want to welcome our witnesses today, and I look forward to our discussion.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF REPRESENTATIVE NICK SMITH

The type of computer systems that banks, universities, government, the military, and large corporations depend on, are immense and extremely complex. It saves time and money the more closely connected a system is internally, and to external systems that it needs to interact with. Because the usefulness of computer systems depends in large part on interconnectedness, they are vulnerable to outside "hackers" who can take advantage of the level of openness that the system must maintain in order to be effective. In addition to the threat of electronic attacks, we must not lose sight of the physical security of central servers.

So the need for a highly trained cyber security workforce is obvious. And in some ways, the work that the Federal Government needs to do in this area is similar to what we are doing to ensure that we produce a sufficient number of workers with technical skills and a math and science background. A few examples of these similarities include supporting the development of innovative new strategies for exciting kids about math and science in K–12 schools, providing funding so that universities and community colleges can take the math and science talent developed in those K–12 schools and focus it towards specific areas of focus, and helping post-graduate programs attract and educate enough talented students to meet growing workforce needs.

But it seems to me that training this workforce gives us a paradox similar to the one that developers of computer systems face in making sure that they are open enough to be effective, but not so open that hackers can take advantage of them. In order to defend a network it is necessary to know how it works and where its vulnerabilities lie. If we want to maintain a cyber security workforce large enough to meet growing need, this information needs to be made widely available. By facilitating this, we make it easy for someone with sinister intentions to obtain the training that he or she would need to wreak the kind of havoc that we are trying to prevent. As we move forward in the area of cyber security education, this is an issue that must be addressed.

Chairman BOEHLERT. Thank you very much.

And our witnesses today, a very distinguished list of witnesses, I want to thank you in advance for agreeing to be facilitators and educators for this committee. We take great pride in the quality of witnesses that are invited before this committee, and we also take great pride in the fact that more often than not we listen. It is easy for the elected officials like us to sit up here and pontificate and talk a lot, but we don't learn much when we are talking. We learn

an awful lot when we hear from people like you. And it is a very diverse panel.

Mr. Chet Hosmer, President and Chief Executive Officer for WetStone Technologies, Inc. in Cortland, New York. Mr. John Baker, Director, Technology Programs, Division of Undergraduate Education, School of Professional Studies in Business and Education, Johns Hopkins University. Mr. Erich Spengler, and for the purpose of an introduction, the Chair will recognize the distinguished Chair of the Subcommittee, Ms. Biggert.

Ms. BIGGERT. Thank you, Mr. Chairman, for the opportunity to introduce Mr. Erich Spengler.

With a Master's degree in Business from Loyola University, Mr. Spengler is the Director of the NSF Regional Center for the Advancement of Systems Security and Information Assurance at Moraine Valley Community College in Palos Hills, Illinois. While the school lies just outside my district, I am here today because Mr. Spengler is almost a constituent and because Moraine Valley truly is an educational asset to the entire Chicago land area, and I think that he is to be congratulated for all that he has accomplished at Moraine Valley and certainly has contributed and will contribute this morning to our discussion of cyber security education. And that is why it is my privilege to welcome Mr. Spengler to the hearing of the House Science Committee today.

Thank you, Mr. Chairman.

Chairman BOEHLERT. Our next witness is Second Lieutenant David Aparicio. Lieutenant, it is good to see you here. He has got an exciting story to tell. Lieutenant Aparicio is a graduate. As a matter of fact, he was the valedictorian of the Advanced Course in Engineering Cyber Security boot camp, and, boy, that is an interesting story, Mr. Gordon and my colleagues, I want you to hear about. And he is joined to his rear by Dr. Kamal Jabaar who is director of the cyber security boot camp. Doctor, it is good to have you here with us. And Mr. Aparicio, I can't resist the temptation. As you probably know, this weekend the most important event taking place any place in the world is taking place in my home district of New York. Cooperstown, the National Baseball Hall of Fame, it is the induction ceremony this weekend. A couple of greats from the past, Dennis Eckersley and Paul Molitor, are being inducted. But one of the popular inductees of many years ago was Louie Aparicio, and so I just want to say it is good to see another Aparicio here.

And for the purpose of an introduction, the Chair recognizes Mr. Gordon.

Mr. GORDON. Thank you, Mr. Chairman.

It is my pleasure to introduce Ms. Sydney Rogers who is Vice President for Community and Economic Development at Tennessee State Technological Community College. I also want to welcome her as a fellow graduate of Middle Tennessee State University and thank her belatedly for voting for me for student body president some years back. Ms. Rogers is responsible for workforce development, student services, computer services, and grants, and development at Nashville State Technical Community College. Previously, she served as interim Vice President for Academic Affairs, Dean of Technologies, and Department Chair and Associate Professor for

Computer Information Systems for 20 years. Of particular interest for today's hearing, Ms. Rogers is the lead principal investigator for the Center for Information Technology Education, a regional center funded by the National Science Foundation Advanced Technology Education Program. Her work has focused on the reform of technological education to create a more adaptable workforce suited for the new century. Ms. Rogers serves on three NSF national visiting committees and several local Boards and has 30 years of leadership experience in technology education and workforce development.

Once again, welcome to our committee.

Chairman BOEHLERT. Thank you very much, Mr. President.

And now the witnesses. And the general rule in the Committee is that we ask that you summarize your opening statement, which will be made part of—the full opening statement, part of the official record in its entirety. But we ask for the summary in five minutes or so, and the Chair is never arbitrary, because in addition to the very distinguished witnesses we have today, we are used to hearing from Nobel Laureates and astronauts and I can't help but recall yesterday was the 35th anniversary of the Apollo 11 Moon landing. We have had Neil Armstrong, with whom I had a good conversation last night, and Buzz Aldrin. And so to have people travel from afar and offer expert testimony, it seems to me sometimes almost sinful that we ask you to summarize in 300 seconds or less. But while the clock will be on, and at four minutes it will— the little sign there will be yellow and in five minutes, it will go red, don't stop mid-sentence, mid-thought, mid-paragraph. Continue on. There will be some leeway, and then there will be opportunity for questions.

With that, Mr. Hosmer, it is a pleasure to welcome you here.

STATEMENT OF MR. CHESTER "CHET" HOSMER, PRESIDENT AND CEO, WETSTONE TECHNOLOGIES, INC.

Mr. HOSMER. Thank you, Mr. Chairman and Members of the Committee, for the opportunity to speak with you today on a topic that is very, very important to me personally and to our company.

For many years now, since 1998, we have been involved in cyber security research and development at WetStone Technologies, and a critical part of that process has been the integration of and cooperation between many colleges and universities throughout our great State of New York. Congressman Boehlert, the Chairman, and myself, actually, are both alum of Utica College of Syracuse University. And that program in economic crime investigation that was started there back in 1988 is one of the oldest in the country in this particular area. And it was at a time where it took great vision in order to be able to create a program in an area where, at the time, no one knew we really had a problem. And we have been working with that program and with the program at Tompkins Cortland Community College to develop programs that can basically better prepare our young people for careers in cyber security.

I can't stress enough how important it is for our cooperation between business and industry and colleges and universities in order to be able to build and structure these programs. The reason is that as you look at this field of study, it is emerging and it is

changing on a daily basis. And sometimes we call it, at Internet speed, the threat and the cyber weapons that are against us are changing. Therefore, the curriculums that have to be provided for those students that are coming up in this particular area need to be flexible. They need to be expandable. They need to be modifiable. They need to be able to be delivered in multiple forms.

So we kind of took an approach to try to work with those colleges and universities to help develop those programs. And I am happy to say that we think it has been a great success. Many members of our staff have spent countless hours actually teaching in those programs as adjunct faculty. And we believe that brings a lot, both to the students and the faculty at those universities that we work with. And one of the real primary objectives of that relationship between our staff and our people and the universities is to build internship programs for those students to be able to move into this field of study.

I can't stress enough how important internships are to this process. The reason is that at a university or a college level, a lot of theory is taught. But unfortunately, in this particular area, practical experience is absolutely essential. One of the reasons is that cyber security, especially in the form of digital investigation, requires knowledge both in the social sciences as well as the computer science area. And the bridging of the gap of those two things requires a great deal of work, because they tend to be taught in two different areas of most universities and colleges. So our ability to bridge that gap, to bring social scientists and computer scientists, criminal justice and computer science folks, together is absolutely critical in order to advance this. And we have done that through internship programs.

I am proud to say that we have been able to hire 14 interns over the last 3¼ years at our company from Utica College, Tompkins Cortland Community College, Syracuse University, Binghamton University in order to bring those into our organization. Over half of them have been offered and accepted full-time employment with our company after graduation. Many others have gone on to other careers in law enforcement, intelligence defense, and corporate security. And our ability to be able to continue that program, to be able to advance that educational model of internship, is absolutely critical.

There are many programs out there that are being trained by vendors, by folks that are in the commercial sector that are providing training for folks that are already in law enforcement, in cyber education, and cyber security that have to go on afterwards. And that training is very expensive. It does not end after graduation from college. In many cases, the folks that are actually on the front lines protecting us on a day-to-day basis are law enforcement professionals that actually did not come up through the computer science track. They actually came up through the criminal justice track. But now, virtually every case that they work with involves some sort of cyber or computer evidence or computer investigation is required. So they have had to go back and take courses in order to basically bring themselves up to speed to be able to do this kind of investigation.

I want to tell this committee that every single week we get requests from those individuals to come to our training courses that are seeking education, and in many cases, those young men and women that are in those services are paying for that training themselves. They are taking time off from their job using their vacation to basically go get trained in this area, because it is that important. They are giving up time with their family and their hard-earned money in order to be able to perform that training, and it is something that we need to support them with.

So I have many more things to say, but I am going to yield to the next member, and I appreciate this opportunity to convey some of the thoughts and some of our experience.

[The prepared statement of Mr. Hosmer follows:]

PREPARED STATEMENT OF CHESTER HOSMER

Mr. Chairman and Members of the Committee: My name is Chester Hosmer; and I am a co-founder and the President and CEO of WetStone Technologies, Inc.

I would like to thank you for the opportunity to testify regarding Cyber Security Education. This area has been, and continues to be a focal point of our work at WetStone from many perspectives. I will focus my remarks on our practical experience with Cyber Security Education as an employer, educator, and trainer, and I will limit my focus to the areas that we are intimately involved in digital investigation and cyber defense. I hope that our "hands-on" perspective will provide an interesting frame of reference for this committee.

WetStone was established in 1998 and is headquartered in Cortland, New York. We perform advanced research and development in cyber security for government and corporate customers. We also develop commercial software products that aid in digital investigation and cyber defense, and we provide advanced training for digital investigators. During the past two years, our focus has been on cyber security training which includes advanced courses in Steganography and Malware Investigation, two technologies used extensively by cyber criminals. During that time we have delivered training to over 1,000 federal law enforcement agents, DOD information warriors, State and local law enforcement investigators and corporate security professionals. The demand for training in these advanced areas has grown rapidly over the past two years to the point where we are typically conducting two or three trainings per month, both in our Cortland training facility, in conjunction with cyber security conferences and at customer's on-site locations.

What knowledge and skills are currently needed in the cyber security workforce?

Those tasked with investigating cyber crime or defending against cyber threats require knowledge of the domain, specialized skills and practical experience. The need is currently both wide and deep. A thorough basis and understanding of investigation techniques either from a criminal justice or law enforcement background, or a formal education program is required. However, when investigating cyber crime, a strong operational and procedural technical knowledge rooted in the computer science field, is also necessary. Unfortunately, most Criminal Justice university programs are offered out of the Social Science departments at universities, where Computer Science a hard science, out of the math or computer science departments. Building programs that cross domains is quite difficult for many reasons, and the student typically lacks depth in either area, and is ill prepared for digital investigation after graduation. We are however, beginning to see an increase in specialized Computer Forensics programs which give students the background necessary for advanced digital investigation.

Many of the current investigators have come through the traditional law enforcement track and learned basic investigation techniques by working task force assignments (narcotics, homicide, child exploitation, etc.). As their cases began to include more and more computer based evidence, the investigators sought training programs that would allow them to seize, extract, examine, analyze and give related testimony about digital or cyber evidence.

Many colleges and universities are attempting to meet the needs of the cyber first responder by offering evening classes or special workshops. However, the colleges and universities are not equipped to offer the advanced "hands-on" training courses needed. In many cases to properly teach these skills, special technology, dedicated

laboratories, field knowledge, and extensive preparation is required. Further complicating college based offerings, is the rapid evolution of both the cyber threats and the defenses necessary to counteract them. This instability in curriculum content makes it very difficult for colleges and universities to develop programs under traditional models.

Have cyber security education and training programs been sufficiently flexible to respond to these needs as well as the needs of traditional and returning students?

The current state-of-the-art of cyber security education and training is varied. Many colleges and universities are now offering both courses and curriculums that range from Junior colleges programs offering A.A.S. degrees, undergraduate education offering B.S. and B.A. degrees, and graduate degree programs offering both Master's and doctorial degrees that relate to cyber security. I have personally been involved in three specific programs being offered at two colleges. At Utica College of Syracuse University, I have been privileged to teach in both the Economic Crime Investigation undergraduate program, and the Economic Crime Management Master's level program. Currently, I serve as the Director of the Computer Forensic Research and Development Center at Utica College and I guest lecture in both the computer security and computer forensic classes. At Tompkins Cortland Community College (TC3), a Junior college of the State University of New York, I had the pleasure of working with the administration and department heads to help establish the first Associates Degree program in Computer Forensics in the United States, and I continue to guest lecture in this program today.

Many commercial vendors are offering training programs that typically relate to their own specialized technology or product and service offerings. In most cases these classes are cost prohibitive for individual purchase and often place a hardship on limited department budgets. Training programs of this type vary widely in price, however a good rule of thumb is about $750–$1,000 per day not including expenses. Advanced training courses typically run 2–5 days in duration. Investigators spend about 1–2 weeks per year on the training required to keep up to date with the state-of-the-art. Compounding the high cost of the training itself, is the time required away from the job. Those working in more rural communities must incur additional travel expenses on top of the high cost of the training. Since these costs recur every year based on the rapid changing landscape of cyber security, a minimum investment of $25,000 to $35,000 per year, per investigator is necessary. Distance learning would seem to be an obvious option that could mitigate some of these costs. This does offers a promise for the future, however, to date only a handful of cyber security training courses are offered in this manner and additional study, research and development is needed.

What are the current strengths and weaknesses in cyber security education and training programs?

Strengths—During the last several years new college based curriculums have been developed to address the demand for cyber security professionals. These programs are being offered at every level of secondary education, and the expertise of the faculty and curriculum development continue to rapidly advance. Options for Associates, Undergraduate and Graduate degree programs offer both new students and those wishing to advance their careers several options from which to choose. Also, many of these curriculums are offered in a "continuing education environment," allowing those currently working to participate as well.

Training offered by private companies, and conference and workshops are providing excellent content today. This type of training has many positive characteristics. First, the content tends to be well aligned with the current threats and solutions due to the competitive nature this environment offers. In addition, the quality of both the trainers and content is sound due to the demand of customers, organization members or conference participants. We see this clearly as the largest area of expansion over the past several years. Conference participants can now attend advance training course, receive college credits, take examinations for industry certifications, stay abreast of emerging trends and network with colleagues during a typical five-day conference.

Weaknesses—Although the education programs have quickly ramped up to develop curriculums and degree offerings to help meet the needs, the graduates of these programs require significant training on practical cyber security matters after graduation, and throughout their careers. In addition, typical college and university based programs have a difficult time staying abreast of current trends. Unfortunately, in the business of cyber security, the trends are changing so rapidly that crafting curriculums to meet the needs is a challenge. This not only goes to the curriculum, but

also the tools and technologies and expensive laboratory equipment and software necessary to expose the students to the latest methods.

The majority of the training programs currently being offered to provide practical skills by both private and non-profit organizations are non-standardized, ad hoc and mostly difficult to qualify or assess. This makes the selection of these programs for training extremely difficult, and the satisfaction level of the attending student low. Unfortunately, due to the rapid evolution in the cyber threat, training is a recurring consideration for both new hires and veteran employees. No uniform certification process for training courses or trainers is in place today to help assess the quality and/or value of the training programs offered. Many organizations utilize colleges and universities to "accredit" their course offerings and deliver continuing education credits to those that complete the training classes. Students then have a number of CEU credits from a variety of colleges and universities with no way to combine those for a degree. In many cases students end up with 100's of hours of seemingly unrelated course credit, when in fact they have acquired more knowledge than most four-year college students attending a traditional academic program.

Do model programs exist and, if they do, are they being adapted to meet local cyber security needs?

The National Security Agency (NSA) has created *The Centers of Academic Excellence in Information Assurance Education (CAEIAE)* program. Established in November 1998, this endeavor helps NSA partner with colleges and universities across the Nation to promote higher education in Information Assurance (IA). This program is an outreach effort that was designed and is operated in the spirit of Presidential Decision Directive 63 (PDD 63), the Clinton Administration's Policy on Critical Infrastructure Protection, dated May 1998. The program is now jointly sponsored by the NSA and Department of Homeland Security (DHS) in support of the President's National Strategy to Secure Cyberspace, February 2003. The goal of CAEIAE is to reduce vulnerability in our national information infrastructure by promoting higher education in information assurance (IA), and producing a growing number of professionals with IA expertise in various disciplines."[1] In New York, Pace University, Polytechnic, SUNY Buffalo, SUNY Stony Brook, Syracuse University and the U.S. Military Academy, West Point have been certified.

Numerous options for training are available at the federal level, including FBI Quantico, the Federal Law Enforcement Training Center (FLETC), the Secret Service Training Center and many others. State and local law enforcement typically with smaller budgets, receive training from private for profit or non-profit organizations such as the High Technology Crimes Investigation Association (HTCIA), InfraGard, the National White Collar Crime Center, the National Law Enforcement Training Center (NLETC) along with many others. In many cases the investigators and officers pay for membership and training out of there own pocket. At WetStone we have first hand experience with this phenomena and receive multiple requests weekly to attend our training by these individuals paying with their own funds to stay current with the emerging threats.

What partnerships should two-year and four-year colleges and universities forge with business and industry to build appropriate programs? In your opinion, is there sufficient collaboration with industry at the administration (advisory committees), faculty (return-to-industry) and student (internship) levels to accommodate rapid changes in these professional and technical areas?

The experiences over the course of my 20+ years in this industry, both in and out of the classroom have provided me with a very interesting perspective regarding not only the needs but the progress that has been made. First, I must say that the young men and women seeking education in these areas are some of the best and brightest I have had the privilege to work with. I learn more every time I enter the classroom either in an academic or training setting than I could possibly repay. During the very early days of WetStone, we launched an aggressive internship program for those working on degrees in cyber security. This program is still in full swing today. The idea was two fold, first to be directly involved in the education process by teaching in the classroom; and second to provide internship opportunities for students that had interests in pursuing a career in cyber security research and development. I am happy to report to this committee that this approach has been a stellar success. To date we have executed 14 internships in cyber security, involving students from every college level. Over half of these students have accepted full-time employment with our company after graduation. In addition to the internships at

---

[1] http://www.nsa.gov/ia/academia/caeiae.cfm

the college level, in June of 2003 we initiated a high school internship program for high school juniors and seniors considering a career in cyber security. Our first high school intern Jeff Olson of Cortland High School is with us again this summer. Jeff graduated in June and will be going on to the Rochester Institute of Technology RIT where he will be studying computer engineering. Based on the success of the high school program we are expanding this internship in the fall to include two additional high school students.

The advancement and availability of education, training and internship programs is paramount if we are to strengthen our nation's cyber security workforce. For example, education at the undergraduate level must include practical as well as theoretical aspects. In this field of study, the state-of-the-art is changing daily and those engaged in education must keep abreast of current trends (technological, legal and operational). In addition, I believe it is important that internships should be a requirement for those working in this field. Without functional internships students graduating will continue to lack practical skills that are a requirement for success. This recommendation should not be taken lightly. A serious commitment by the student, the college or university, and the private sector is necessary to make this endeavor successful. One metric that we have developed for our own cyber security internship program is the 2-for-1 rule. For every two cyber security interns we hire, we need to dedicate one-full time staff member to direct and mentor the interns— a significant commitment for large or small companies. In many cases employers consider only the labor cost of the interns when making an intern program decision, when in fact the cost is many times higher. However, long-term commitments are necessary, and your ability to mentor these students during their junior and senior years will pay significant dividends after graduation—as they step directly into the organization and begin producing and contributing immediately. Also, the colleges and universities are required to commit staff hours to monitor the process the internships in the field. These monitors need to be selective as to the environments that students consider—again requiring extensive planning and follow-up for an already overloaded schedule. However the payoff here again can be considerable. By interfacing directly with prospective employers, educators are able to identify gaps in their curriculum, get feedback as to the student's preparation, and directly improve the overall programs.

Colleges and universities must forge partnerships with both the public and private sector. In my opinion the internship model is one that should be considered. This model provides all the elements necessary to better prepare students for the workforce and to garner direct feedback throughout the life cycle of the cyber security curriculum development. As new issues and threats are revealed, this feedback will be focused and swift. The internship opportunities also allow the colleges and universities to build relationships with employers that will better define and characterize the jobs these new cyber warriors take on. This understanding will again help shape the curriculum as a whole, along with shaping the syllabus of specific courses. One other benefit of this approach will be the access to local experts that are willing to guest lecture in the classroom. These local experts educate everyone in this environment (professors, students and colleagues) not to mention what they may learn while interacting with the next generation workforce. I realize that in writing this one may think there must be and easier way, because this sounds like hard work. Unfortunately, I'm not sure there is a silver bullet, as the responsibility for advancing the cyber security of the country should fall to everyone's shoulders. In almost all cases, we have forged these relationships—one student, one professor, one college, one department head at a time. We must all take a passionate interest in advancing our capabilities against the ever increasing cyber threat and get our hands dirty, and give back what we learn and know about every aspect of this threat. Today, the criminals and terrorists communicate and they share information about weaknesses, system vulnerabilities, our critical infrastructures, social engineering, stolen passwords, credit card numbers, malicious code and the latest cyber weapons freely and virtually unchecked over the Internet. We must do the same. And I believe education and training are the basis and the first critical step. At WetStone we adopted a quote as our company's vision in 1998. The quote came from a different time when our nation was facing a different adversary, but as often happens, the words of great men withstand the test of time. Robert Kennedy said in 1960, "If we do not on a national scale attack organized criminals with weapons and techniques as effective as their own they will destroy us." By dedicating ourselves to the transfer of knowledge in cyber security to those that are defending, or will defend us, we can train the workforce of the future and begin making a difference today.

What can the Federal Government do to improve cyber security education and build the Nation's technical workforce?

I feel that the Federal Government can have direct impact on the advancement of education and training in cyber security from several perspectives.

First and foremost, cyber security training and education can be made more accessible to our men and women in law enforcement who today can only advance their education and training in this area by spending their personal funds, trading their vacation time, or giving up time with their families to attend a training course that will ultimately help them defend our nation. Offering them assistance to participate in qualified education and training programs will accelerate the process for those already investing in our future and encourage those that today do not have access.

Second, incentives to colleges, universities and the private sector to create internship opportunities in cyber security can be increased. The cost required to carry out this endeavor is staggering today, however, in my opinion this is an investment that we cannot afford to overlook.

Third, national accreditation of cyber security education and training programs that would allow those to combine credits and experience to obtain higher education degrees in a flexible, fair and non-traditional form is urgently needed. We need to not only attract today's young people entering college into this field, we must also encourage those that have many years of street experience in law enforcement to gain the recognition based on their years of investment in our future. When they step on the street tomorrow, they may encounter "cyber evidence" that could in-fact hold critical information that would preempt a crime, a pending terrorist action, or the exploitation of a child. Their preparedness, I believe, should be our paramount concern.

I would like to thank the Committee for this opportunity to present my experience, thoughts, views and perspective on cyber security education and training.

BIOGRAPHY FOR CHESTER "CHET" HOSMER

Chet Hosmer is a co-founder, and the President and CEO of WetStone Technologies, Inc. He has over 25 years of experience in developing high technology software and hardware products, and during the last 15 years, has focused on research and development of information security technologies, with specialty areas including: cyber forensics, secure time, and intrusion detection and response.

Chet is a co-chair of the National Institute of Justice's Electronic Crime and Terrorism Partnership Initiative's Technology Working Group, and was one of five international steganography experts interviewed by ABC News after the 9/11 al-Qaeda attacks. Chet has been quoted in numerous cyber security articles, and has been invited to present as both a Keynote and Plenary speaker numerous times over the course of his career.

Chet is a member of the IEEE and the ACM, and holds a B.S. degree in Computer Science from Syracuse University. Chet is also the Director of the Computer Forensics Research and Development Center of Utica College.

Selected Publications and Speaking Engagements:

"Steganography Detection: Finding Evidence in Plain Sight," 15th Annual ACFE Fraud Conference and Exhibition, July 12, 2004

"Scanning-Detecting-Eradicating—and Recovering from the Malware Invasion," Techno Security 2004, June 8, 2004

"Time: The Missing Link in Digital Integrity," Gorham International Conference, May 25, 2004

"Bigger Than Viruses-How Malicious Software Can Affect Your Business," Tech 2004, May 4, 2004

"Discovering Evidence Hidden In Plain Sight," Southeast Cybercrime Summit 2004, March 3–4, 2004

"Biometrics and Digital Evidence" with Countryman, B. *The Security Journal,* Winter 2004, Volume 6

"Protecting the Homeland using Biometric Identification," Sector 5—The Global Summit Exploring Cyber Terrorism and the Targets of Critical Infrastructures, August 21–23, 2002

"Steganography Detection: Finding Evidence Hidden in Plain Sight," Forum on Information Warfare, December 2003

"Applying Hostile Content Detection to Digital Forensic Investigation," *The Security Journal,* Fall 2003, Volume 5

"Cyber-Terrorism: Digital Steganography and its Implications for Homeland Security," Securing the Homeland Conference & Expo, September 10, 2003

"Steganography as It Relates to Homeland Security," Electronic Crimes Task Force Homeland Security Seminar, September 4, 2003

"Discovering Covert Digital Evidence," DFRWS Conference, August 6, 2003

"What You Can't See Can Hurt You—The Dangers of Steganography," *The Security Journal,* Summer 2003, Volume 4

"Digital Steganography: The Evolving Threat," Techno-Security 2003, April 29, 2003

"The Importance of Digital Time in Preventing Economic Crime," *CyberCrime 2003,* February 9, 2003

"Tracking Cyber Criminals With Time," NATO Inforensics and Incident Response Workshop Keynote, October 22, 2002

"What You Can't See Can Hurt You," *SC Magazine,* August 2002

"Proving the Integrity of Digital Evidence with Time," *International Journal of Digital Evidence (IJDE),* Spring 2002, Volume 1, Issue 1

"Steganography Detection: Finding Evidence Hidden in Plain Sight," Techno-Security 2002, April 10, 2002

"The Importance of Binding Time to Digital Evidence," 12th Annual Economic Crime Investigation Institute Conference, October 30, 2001

"Technical and Legal Issues in Network Intrusion Investigations," with W. Williams and A. Ott, October 31, 2000 11th Annual Economic Crime Investigation Institute Conference. Cyber Swords and Shields Fraud Symposium, October 3–5, 2000

"State-of-the-Art of Computer Forensics," 10th Annual Economic Crime Investigation Institute Conference, November 9, 1999

"Advancing Crime Scene Computer Forensics Techniques," with J. Feldman and J. Giordano, SPIE's International Symposium on Enabling Technologies for Law Enforcement and Security Conference, November 1998

"Using SmartCards and Digital Signatures to Preserve Electronic Evidence," SPIE's International Symposium on Enabling Technologies for Law Enforcement and Security Conference, November 1998

"System Modeling and Information Fusion for Network Intrusion Detection," with N. Ye, J. Feldman, and J. Giordano, ISW '98, October 1998

"Detecting Subtle System Changes Using Digital Signatures," with M. Duren, 1998 IEEE Information Technology Conference, September 1998

"Time-Lining Computer Evidence," 1998 IEEE Information Technology Conference, September 1998

"The Role of Smart Tokens in Cryptographic Key Management," with P. Samsel, *PARAPET Journal of Information Security,* Autumn 1997

"Controlling Internal Fraud: Detection and Countermeasures Using Intelligent Agents," Economic Crime Investigation Institute Eighth Annual Conference, Oct. 27–28, 1997

"Developing Solutions That Employ Tamper Proof Token Devices to Protect Information Integrity and Privacy," IEEE Dual-Use Technologies and Applications Conference, May 1997

"Securing Lottery Electronic Instant Ticket Technology," with M. Holcombe, 1994 National Lottery Technology Conference, November 1994

Media Coverage

"Secret Codes": NHK Japan Television, December 2002

"A Novice Tries Steganography"—Tech TV—Cyber Crime Show, January 2002

"A Secret Language"—ABC News Prime Time Thursday, October 4, 2001

WetStone
Securing Digital Integrity

July 19, 2004

The Honorable Sherwood Boehlert
Chairman, Science Committee
2320 Rayburn Office Building
Washington, DC 20515

Dear Congressman Boehlert:

Thank you for the invitation to testify before the U.S. House of Representatives Committee on Science on July 21st for the hearing entitled, **Cyber Security Education: Meeting the Needs of Advanced Technology Workers**. In accordance with the Rules Governing Testimony, this letter serves as formal notice of the federal funding WetStone currently receives, and has received in the past in support of our research.

- Contract Title: Cyberscience Lab Applications
  Amount: $314,679
  Contract Type: Subcontract with Dolphin Technology, Inc.
  Prime Contract: AFRL - FA8750-04-C-0103
  Awarded: FY04

- Contract Title: Malicious Code Sentinel – Steganography Detection
  Amount: $149,997
  Contract Type: Subcontract with Orincon Corporation
  Prime Contract: AFRL - F30602-02-C-0055
  Awarded: FY03

Sincerely,

Chester D. Hosmer, Jr.
President & CEO

Chairman BOEHLERT. Thank you very much.

You will be interested to know that you were only 45 seconds beyond the five minutes.

Our next witness, Mr. Baker, is accompanied by a support staff, his young son, Chris, who is behind him in the audience and who is working on a scouting merit badge in citizenship. So what we are talking about here, in many respects, is dealing with human capital for the future. So I am glad to see Chris here with you, Mr. Baker.

STATEMENT OF MR. JOHN R. BAKER, SR., DIRECTOR, TECHNOLOGY PROGRAMS, DIVISION OF UNDERGRADUATE EDUCATION, SCHOOL OF PROFESSIONAL STUDIES IN BUSINESS AND EDUCATION, JOHNS HOPKINS UNIVERSITY

Mr. BAKER. Thank you, Mr. Chairman.

Thank you for the opportunity to speak today, and as you so eloquently indicated, I am director of the undergraduate programs in technology in the School of Professional Studies in Business and Education at Johns Hopkins University. In that capacity, I run both our undergraduate degree programs in information system with concentrations in both information security and cyber forensics and the public technology training programs that we run.

We define "cyber security" as the process of informing technology professionals, end users, managers, and researchers about the technical and non-technical aspects of protecting their information resources and expanding our knowledge in the field. As I indicated before, it is a multidisciplinary approach. It has both breadth and depth, including math, science, technology, business, law, psychology, and personal issues. It includes topics that range from simple virus protection to a lot more elaborate forms of security technology detection, investigation, prevention, as well as many non-technical areas. In addition, its audience includes end users, technology professionals, managers, and researchers. Consequently, information technology—information security education necessarily covers a wide range of topics at a variety of levels.

In addition to the specific topics, programs in the area must address issues such as the demand for graduates, the differences between training and education, program development, faculty hiring and development, research, and developing the field as its own discipline, and recognizing and accepting educational standards, and keeping costs manageable while keeping programs current and the potential for student background checks. To ensure program success, the educational institution must have some understanding of the need or demand for program graduates. Potential students with little or no employment opportunities will not select any given program.

In the area of education and training, a strong differentiation between the two must be understood. Training is generally focused on product or a specific set of skills in an area. Education's goals are multi-purpose: teach the specific technology skills, develop critical thinking and problem-solving skills, improve the knowledge of the field, improve communication capabilities and information literacy skills, and foster research interests.

As for program development, it is both costly and time-consuming. It can take a year or longer for a program to be fully developed and implemented. There are many questions to be addressed in the development and implementation of a program and steps to be worked through.

Faculty is a key to a program's development and success. Questions such as the role of full-time and part-time faculty, faculty knowledge and development, and the role of research are constantly being addressed. Each requires considerable analysis.

One way to encourage involvement in the field is to define it as a discipline. Components of this include the availability of research money and the development of educational standards, especially as they relate to employment opportunities.

As with all such endeavors, cost is an important factor. Costs obviously include the specific technology components, however, they also include facility set up, management and maintenance, aca-

demic program development, implementation and management, faculty hiring and development, and the potential for other components, such as background checks.

A more recent issue that has surfaced is this issue of student background checks. Some have expressed concern that we may need to determine the suitability of a student for these types of programs. However, there are many questions to be addressed before this issue can be resolved. Johns Hopkins has taken an institution-wide approach to both education and research components.

Our academic community has developed educational components and/or degree programs that span almost all disciplines and topics in the information security field. Johns Hopkins has created the Johns Hopkins University Information Security Institute, implemented security education in all of its schools, created separate academic programs and program collaboration specifically for information security and cyber forensics, and encouraged research in a number of security-related areas. The undergraduate program in our school focuses on both sides of the security incident before and after the security preparation and cyber forensics.

There are some areas the Federal Government can be of assistance: include more complete funding for the NSF initiatives, encourage the development of educational standards, work with private industry and state governments to provide scholarship opportunities for their potential employees, and assist some government agencies in absorbing the graduates of the Scholarship for Service Program.

More information on these are provided in the detailed testimony I have submitted to the Committee separately. I would like to take this opportunity to again thank you for this opportunity to speak to the Committee.

[The prepared statement of Mr. Baker follows:]

PREPARED STATEMENT OF JOHN R. BAKER, SR.

1. Cyber Security Education

Cyber Security Education is the process of informing technology professionals, end-users, managers and researchers about the technical and non-technical aspects of protecting their information resources, and expanding our knowledge in the field. It is a multidisciplinary field that is both broad and deep. The field is constantly evolving to incorporate more components based on current and historical events and research. The term itself refers both to security aspects as well as to cyber forensics. It requires simultaneous education, training and research in multiple areas (technology, business, management, finance, psychology, computer science, etc.)

a. Components of the Field: Technical, Managerial, Operational

Cyber Security Education is more than just the technical aspect of detecting or eliminating the latest virus, or preventing hacker attacks (the public personae). It requires knowledge of technical areas, addressing management, and how to infuse security practices into the everyday operational aspects of an organization. Technical aspects include firewalls, network security, cryptography and software development.

Managerial components include personnel issues, disaster recovery planning, funding (direct and indirect costs, ROI, payback), the psychology or mind-set of a perpetrator, operational security management, public relations and legal/regulatory components. Operational issues include day-to-day security operations, both for the security field professional and the everyday user.

Each part of the field involves varying levels of research, education and training. Research investigates new technologies, financial issues, approaches to security management, personnel issues and legal/regulatory needs. The most recognizable research is on the technological components of information security.

b. Education vs. Training

Often interchangeably used, education and training differ greatly. Education's goal for the student is multi-purpose: teach them specific technical skills, develop critical thinking and problem-solving abilities, increase the knowledge of the vast background material in the field, improve communication capabilities and information literacy skills, and engage the student in some form of research.

Training is generally focused on a product or specific set of skills in an area. However, at its highest level, some training attempts to approximate education, typically by improving some of a student's background knowledge in a field and/or developing problem solving capabilities.

c. Research and Education

A major methodological issue for a university is whether to focus on research or on classroom education. University reputations are based on faculty research and the institution's research abilities. Johns Hopkins University was the first U.S. university to include research in the educational process. Typically, university research has not been focused specifically in the areas of information security or cyber forensics. Research for these areas is done in various other disciplines that directly or indirectly affect these fields.

d. Emerging Discipline

Because of its breadth, Cyber Security Education is a young field and not currently recognized as a discipline. At the moment it has not yet been accepted as a discipline of its own. It has components in various areas: mathematics, computer science, business, finance, engineering, psychology, law, etc. Consequently, research, education and training occurs in each of these disciplines independently. For example, research in the field of mathematics may result in a better crypto-key system.

2. Programs at JHU

Johns Hopkins has responded to the need for intensive research, education and training in cyber security in all of its academic areas. Some of its programs were in place before the events of Sept. 11. However, all schools at the university have implemented or are in the process of implementing, information security education and/or research in their academic disciplines. In addition, Hopkins has created the Johns Hopkins University Information Security Institute whose goals are to foster research in information security, help develop multidisciplinary approaches to security education, provide seminars and other educational activities, and advance the literature in the field.

a. Internal Programs

Almost all schools at Hopkins have incorporated some form of security education. Depending on the program and level, it could include simple background knowledge about the area and how security applies to the specific educational discipline, or it could include in-depth studies into security approaches in a field, practical applications or advanced security research.

b. Internal Collaboration

Several of Hopkins' Schools have collaborated on academic programs that are interdisciplinary in nature. The flagship program at Hopkins' Information Security Institute is the Master's of Science in Security Informatics (MSSI). It is a collaboration of several schools at Hopkins: Whiting School of Engineering, Krieger School of Arts and Sciences, Bloomberg School of Public Health, Nitze School of Advanced International Studies and the School of Professional Studies in Business and Education. Over 25 full-time, part-time or adjunct faculty are available to deliver the MSSI courses at multiple Hopkins' sites in the Baltimore-Washington area.

In addition, some schools at Hopkins have developed internal collaborations across academic levels. The Whiting School of Engineering and the Krieger School of Arts and Sciences jointly offer a concurrent Bachelor's/Master's program in security. The School of Professional Studies in Business and Education offers a joint technology Bachelor's/Master's degree, with a concentration in information security.

c. External Collaborations

The School of Professional Studies in Business and Education is in the process of developing joint programs with several area community colleges. These would provide students at two-year institutions complete academic program opportunities at the Bachelor's level, and extending into the Master's level.

The joint program offered by the Whiting School of Engineering and the Krieger School of Arts and Sciences includes opportunities for undergraduates of other local universities, which have established agreements with these Hopkins schools.

29

d. Research, seminars, courses/teaching, publishing

The Johns Hopkins Information Security Institute has become the focal point for information security research at the university. Over 15 full-time faculty or JHU Applied Physics Laboratory researchers are involved in some aspect of information security research.

3. Strengths & Weaknesses of Current Education

a. Education or Training

Often a potential employee seeks the short-term goal of satisfying a potential employer's advertised need, through specific skill-set training. Many potential employees view the requirements indicated in a particular employment ad, then attempt to obtain the specific skill required (CISCO training, CISSP certification, etc.). While potentially valid as an entry into the field, or for specific job requirement, these are not intended to indicate the wider-range of skills and abilities many employers seek.

Education rather than training provides potential employees this wider-set of knowledge and abilities, in addition to specific technology skill sets (not necessarily for a specific product). These include: critical thinking and problem-solving, knowledge of the vast background material in the field, communication, information literacy and some form of research. Often a student in a program wants to know if they will be learning Product-X. The answer is usually that the program may teach you some things about Product-X, but its goal is to teach you how to learn, and apply that skill to learning about different products. At times we may use various products (including Product-X) as examples in our classes or for demonstration purposes, but the goal is not to teach a specific product.

In addition, education is intended to develop the next generation of researchers in a discipline. Because of the nature of the information security field, much of the research is focused in other disciplines. For example, a math researcher may apply their findings to the information security field.

b. Costs:

The cost of education programs covers many components: physical items, facilities management, program development and maintenance, and faculty hiring, training and education.

1. Facilities Set-up and Management

Teaching state-of-the-art information security or cyber forensics programs requires facilities that can handle the technology. This means some form of computer lab capability, typically networked. While the most current technology is not absolutely necessary, the more dated the technology the more difficult it is to get current and potential students and employers to accept a program as useful. It is a constant problem to remain current enough to teach the most important components of security and forensics, and still not spend 'every last dime' on the most recent technology.

An additional component is the style or set-up of lab facilities. Most lab set-ups will be done in one of two approaches: a dedicated lab or a multi-purpose lab. Dedicated labs are designed for a specific program, and have minimal impact on other programs or facilities. However, they will sit idle when the specific educational program is not offered. In addition, management of these labs may be easier (for program setup and use), but they are almost always 'locked down', and only allowed for students of the specific program. No other use is allowed because of the sensitive nature of the set-up, and because of the potential problems with other areas. For example, if a lab virus or other destructive software is unintentionally allowed into another lab facility, that facility may become corrupted. If it is a networked facility, others may also become corrupted.

Multi-purpose labs are more functional, but can be much more costly in terms of set-up and management. These labs may need periodic isolation, a special set-up, and additional management. In addition, when they are used by the security or forensic program, disruption to other programs needing the lab will occur. This will include specialized set-up and clean-up time, in addition to the actual class time.

All of these take time, resources and increase costs of program offerings. Hardware costs can range from $500 to $2,000 per machine, plus networking and software costs. Management time will include initial lab set-up, in addition to the individual class set-up and clean-up, depending on the type of lab. While difficult to provide specific cost estimates for this time, it can include several hours of a lab manager's time and up to 1½ days of a support staff person's time, for each class session.

2. Program Development & Maintenance

Development, implementation, operation and maintenance of an educational program can take more than a year. Typically, the process includes:

    a. An assessment of the need for graduates of a program

    b. Development of an advisory board

    c. Identification of program components

    d. Internal and external approval steps

    e. Organization of the program into modules/courses

    f. Development of the course material

    g. Advertising/marketing the program

    h. Program implementation

    i. Constant program evaluation and improvement.

While there are ways to speed up the process, each step is needed. In approving such programs, cost is always a major factor. Employment surveys, component development costs, hardware and software identification, developing appropriate course/lesson plans around them, marketing and oversight are the major ones.

3. Faculty

Cost issues for faculty center on the issues of part-time vs. full-time faculty, and the role of faculty in the program. Part-time faculty are usually used for teaching purposes, and to provide expertise in a specific topic area. While they may be involved in program development, they are not typically responsible for program development or success/failure.

Full-time faculty are involved in one or more aspects of program development, implementation, teaching, evaluation. In addition, in many institutions they are involved in research activities. This can be a source of cutting-edge knowledge, prestige and income for the faculty member and institution, but can also create problems. These and other faculty issues are addressed in section 4.a.

c. Background Checks

A more recent problem that has surfaced is the issue of student background checks. With the events of September 11, increasingly questions of appropriateness of students in the classroom have arisen. A discussion of background checks raises many additional questions:

    1. What is the purpose of the background checks?

    2. How deep or wide will they go?

    3. How much will they cost?

    4. How long will they take?

    5. Who will pay for them?

    6. Who will do them?

    7. What will we do with the information once it is obtained?

    8. Will it prevent a student from entering a program or restrict their access to certain courses or material?

    9. Are they relevant given the availability of material on the Internet?

    10. Are they legal?

Background checks are costly, time consuming and raise legal concerns around privacy and profiling. But, given the awareness of security concerns, additional guidance will be needed in this area.

d. Ethical Agreements

Some programs have instituted ethical agreements with students in specific programs. They attempt to educate the student on the seriousness of the topic, and the expectations of professional and moral behavior that accompany the education. However, enforcement is difficult, especially outside the classroom or after the program is completed.

4. Faculty Preparation, Recruitment and Retention

a. Part-time vs. Full-time Faculty

Identifying appropriate faculty for specialized programs such as information security and cyber forensics is a challenge. Generally, the options are:

    1. Design the program around the current full-time faculty knowledge base

    2. Upgrade current full-time faculty skills/knowledge

3. Hire new full-time faculty, specifically for this program
4. Hire part-time, practitioner faculty to teach in the program

Designing the program around the current full-time faculty knowledge base is the easiest and least costly approach, but is usually the least desirable. Typically, their knowledge base is very specific and may not cover the broad-range of technical and non-technical topics required. Consequently, the program manager is required to augment the current knowledge base with additional, training or education, or hiring other faculty, either full-time or part-time. In addition, the current faculty knowledge base may already be out-of-date or too narrow.

Upgrading current full-time faculty skills and knowledge is desirable and useful for them, but is time consuming and adds cost to the program development and operation. It may delay the program development and implementation.

Hiring new full-time faculty may be quicker, but also costly. In addition, if the program is not commercially successful (and if they are not involved in research which generates grant income), the organization has incurred the additional faculty cost, with no offsetting income. That may mean the faculty position results in a short-term employment opportunity.

Hiring part-time, practitioner faculty is often difficult and time consuming. While it provides the educational institution the least costly staffing solution, there are many other factors that affect the hiring decision. These faculty often:

1. Are not trained educators
2. Are already employed and consequently have problems with pre-existing course schedules
3. Cannot teach during the day
4. May travel too much
5. May have only some allegiance to the program and/or institution
6. May not have the necessary academic credentials
7. May not have a teaching aptitude

When hiring part-time faculty the organization needs to commit to teaching them to be educators. Learning to educate at the college or university level requires some intensive interaction between the academic program manager and part-time faculty member, and a commitment on the part of the university to provide faculty development in the area of teaching skills and course/classroom management. In addition to creating a syllabus and organizing some lectures, the part-time faculty member will need to learn to manage the classroom environment, create and implement effective and fair evaluation instruments and assign grades. In addition, the faculty will need to evaluate student writing, incorporate critical thinking and problem-solving skills, include information literacy, develop creative presentation styles, and infuse current research into the education process. These can take some time, patience, and commitment on the organization's part, with no guarantee the part-time faculty member will continue with the program.

In addition, the education organization needs to implement a support system for the part-time faculty member. This includes administrative support for typical needs (copying, book order processing, etc.), and academic support for course content, unexpected problems, articulating college/university policies on various issues and handling grading questions.

b. Teaching vs. Research

In some educational organizations, full-time faculty may also be involved in research activities. While this can provide a terrific resource for the program in terms of up-to-date information in the field, and potential student involvement in the research, it can also create conflicts for the faculty. Research activities are often funded by grants and require intensive time commitments of the faculty. Consequently, less time is available for teaching.

c. Hopkins Approach

Hopkins has implemented a variety of solutions to address faculty issues. In some schools, full-time faculty are involved in both research and teaching. In addition, part-time faculty are used in selected courses or program components to either provide the instruction or assist the full-time faculty member with their instruction.

Others schools at Hopkins are using a large group of part-time faculty who are professionals in their area, to teach in their program. In addition to selecting fully qualified part-time faculty (based on factors such as professional experience, teaching experience, teaching aptitude, academic credentials and availability), they are

provided a full range of teaching professional support from both the program manager and other groups with the organization.

5. Federal Government Assistance

a. Funding NSF Initiatives

The National Science Foundation (NSF) has attempted to provide several opportunities to fund information security educational initiatives. Because of funding issues NSF has not been able to support innovative initiatives in information security education. Providing more complete funding for the NSF initiatives will help in the development of different and more complete academic programs.

b. SFS Graduates

Evidently, one of the issues with the Scholarship for Service (SFS) program is the ability of government agencies to absorb the number of graduates. Some may need assistance in developing their plans and/or finding ways to hire the graduating talent. Others, (DOD, NSA, etc.) have indicated a strong need for qualified SFS graduates. One issue here may be the ability of the students to obtain appropriate security clearances.

c. Development as a Discipline

Provide some funding to encourage the development of information security and cyber forensics as disciplines. This would encourage faculty to enter the field, develop research incentives, and provide money for the development applied and research-based academic programs. In addition, it would bring together research and education that is pertinent to the field.

d. Non-SFS Scholarships

Working with the private sector and state governments, the Federal Government can help to develop scholarship programs to provide educational funding for students who may want to be employed in one of these areas. The private sector and state governments have as strong a need for information security professionals as the Federal Government. In some instances they may be on the front lines, or provide early-warning notification to the Federal Government. Consequently, they need as much education in the security area as the Federal Government.

6. Other Issues

In addition to the request information areas, these additional topics may be of interest:

a. Defining Educational Standards

Developing educational standards in a discipline helps define it as a discipline. The defining of such standards would help the fields of information security and cyber forensics. While simple in concept, it is more difficult in practice. It would require the defining of security knowledge needs in various professions, and at different levels within a profession. For example, in a given industry there are system end-users, managers, technical staff and researchers. Each requires different levels and types of security education and skills. The end-user may need to understand how, and a little of why, a password needs to be changed regularly. In addition, the organization may be helped of they are educated about typical security breaches that can occur. Technical staff will need more in-depth education about preventing security problems from occurring, solving unexpected security problems and reporting them to the appropriate people.

b. Traditional-age Students vs. Returning Adult Students

Students in an educational program are typically one of two types, the traditional-age student progressing through the academic process, as we have come to expect, and the returning adult student with several years of work experience. In most instances they are seeking the same result, entry into the information security field, either applied or research. At times they may co-exist in a program. However, typically specific part-time programs are usually offered for the returning adult student. These programs are not usually considered when issues concerning education are addressed.

BIOGRAPHY FOR JOHN R. BAKER, SR.

EMPLOYMENT:

Johns Hopkins University, School of Professional Studies in Business and Education, Baltimore, MD

Director, Undergraduate Technology Programs (July 1999 to present)

Key Responsibilities:

Direct activities for undergraduate degree, certificates and non-credit (training) programs in information and telecommunications technology. Responsibilities include: market assessment, program planning, course development and scheduling, budget management, marketing and strategic planning for academic technology needs. Also assisted in redevelopment of school-wide technology strategic planning, both academic and administrative.

Major accomplishments:

- Worked on team to develop strategic technology plan for entire school for both academic and administrative areas
- Redesigned and implemented innovative undergraduate technology degree (BS/Information Systems) and credit certificate programs
- Redesigned and expanded non-credit (training) programs (CONNECT)
- Manage on-site programs with local organizations

Graduate Faculty (Jan. 1998 to July 1999)

Key responsibilities:

Assist business technology degree program director with program development and operation. Major areas include: course development and quality assurance, faculty development and quality, scheduling faculty assignments and managing graduate technology degree completion course.

Advanced Technologies Group, Columbia, MD (Aug. 1995 to June 1999)

Director, Consulting Services

Key Responsibilities:

Direct activities to identify and secure potential consulting engagements, work with consulting clients, plan and manage projects, provide consulting expertise as needed and assist with business development. Responsible areas include: information systems, technology training, executive education program, telecommunications, technology in education, strategic technology planning, the Internet and World-Wide-Web. Major clients include: AT&T, MCI, SAIC, U.S. Dept. of Interior, World Airways, U.S. Dept. of Veterans Affairs, StorComm Inc., and Amnex Inc.

Johns Hopkins University, School of Continuing Studies, Baltimore, MD (Nov. 1987 to Aug. 1995)

Director, Technology Programs (Nov. 1987 to August 1995)

Key Responsibilities:

Directed activities for large program of graduate and undergraduate degrees in information and telecommunications technology, professional training programs and executive seminars. Responsibilities included: market assessment, program planning, course development and scheduling (over 800 sections and 120 faculty per year), assistance for over 1100 students, budget management, marketing and strategic planning for academic technology needs.

Major accomplishments:

- Designed and implemented innovative graduate technology degree (MS/Information & Telecommunication Systems); undergraduate information systems program; credit certificate education, entrepreneur training and executive education programs,
- Redesign of graduate technology management (MS/Business-Management of Technology), and professional education programs, and
- Finalist for innovative technology impact award in Baltimore.

Director, SCS Operations, Montgomery County Center (Nov. 1987 to Aug. 1990)

Key Responsibilities:

Managed the start-up and operation of the School of Continuing Studies (SCS) remote-campus facilities at the Johns Hopkins University, Montgomery County Center. Responsibilities included: planning and implementation of SCS operations (for

multiple departments), marketing (evaluation, planning and implementation), public presentations, promoted the School and University with county business, education and government. Simultaneously directed graduate business degree concentration in Information Technology Management.

Major accomplishments:

— Started school's most successful off-campus education facility
— Managed growth rate of over 125 percent per year for each of first three years
— Established educational presence in the county and developed links with business

The International Bank for Reconstruction and Development (The World Bank), Washington, DC (Jan. 1984 to Oct. 1987)

Systems and Facilities Manager

Key Responsibilities:

Managed the administrative and investment trading systems and facilities for the Investment Department of the World Bank (a $20 billion investment operation). Responsibilities included: planning and implementation of new information and telecommunication (voice and data) systems, investment facilities and offices; budget management; managing vendor contracts (exceeding $1.5m); system security; strategic technology planning, disaster recovery planning and management; mainframe systems oversight.

Major accomplishments:

— Planned and managed the construction of a new $2m securities trading facility,
— Planned, contracted and implemented a new $1m mainframe computer system,
— Negotiated and managed $3.5m software implementation contracts, and
— Implemented new office automation technology for department of 40 professionals, in multiple locations.

Coopers and Lybrand, Washington, DC (Sept. 1979 to Jan. 1984)

Senior Management Consultant

Key Responsibilities:

Managed and conducted various consulting engagements for the Washington, D.C. office of the Management Consulting Services group. These engagements were for a variety of Federal and State Government agencies, and private organizations.

Projects included:

A security review of the U.S. House of Representatives' computerized Financial Management System; designed and implemented an economic modeling system for the U.S. Department of the Treasury; redesigned the automated central personnel database for the Department of the Navy; managed several engagements to implement, enhance and maintain financial portfolio management software for several state housing agencies, including: Nebraska, New Hampshire, Oregon and South Carolina.

MRI Systems Corporation, Washington, DC (April 1978 to Sept. 1979)

Project Manager

Key Responsibilities:

Managed consulting services contracts for various U.S. government agencies. These were primarily for the development and implementation of management information systems using the SYSTEM 2000 Data Base Management software. Major projects included systems for: Harry Diamond Laboratories (DOD), Mobile Equipment Research and Development Command, the Defense Mapping Agency, and the Department of Agriculture.

Lockheed Electronics Corporation, Houston, TX (Sept. 1977 to March 1978)

Project Leader

Key Responsibilities:

Project leader for a Space Shuttle information system support team—monitored the implementation of operating system enhancements, and implementation, support and modification of all commercial software packages. In addition, the team was responsible for analyzing existing hardware and software utilization and developing new requirements for the Control Data Corporation computer data center at the NASA Space Center in Houston, Texas.

Commercial Credit Corporation, Baltimore, MD (Nov. 1971 to Aug. 1977)

Key Responsibilities:

Held a variety of positions, including: Operations Manager, Data Base Manager, Project Leader, Systems Analyst and Programmer. Major duties included: managing department responsible for the daily operation of an on-line, real-time loan processing system with over 1,000 terminals in 800 offices nationwide; lead team responsible for the control and recovery of a large on-line, real-time financial data base; developed and implemented on-line applications processing system; supervised the programming and design teams which were responsible for user interface, design, programming, testing and implementation of new applications; assisted in the design, programming and implementation of an on-line financial application system processing for over 1 million customers nationwide.

Federal Reserve Bank of Richmond (Baltimore Branch), Baltimore, MD (July 1969 to Nov. 1971)

Senior Systems Operator

Key Responsibilities:

Progressed from operator trainee to senior operator in mainframe IBM systems center. Major duties included: operator for an IBM 360 mainframe, monitoring the quantity and quality of work processed during the shift by junior level operators.

ADDITIONAL QUALIFICATIONS

Johns Hopkins University, School of Continuing Studies, Baltimore, MD (Sept. 1983 to Nov. 1987)

Part-time Faculty

Position summary:

Part-time faculty position assisting in development and teaching in technology program. Planned, designed and conducted beginning and advanced technology courses for students in the graduate Business degree, Economic Education program, graduate Information Systems and Telecommunications degree undergraduate Information Systems degree, and professional development training programs. Topics included: I.S. Management, Strategic Planning for I.S., Advanced Topics in I.S., Applied Graduate Project, Project Management, Business Applications of Computers, Systems Analysis and Design, Business Planning, and beginning through advanced training in: Novell Office Suite, Microsoft Office Suite, Lotus-123, Windows, Internet and World-Wide-Web. Also, continue to assist with curriculum design and development for credit programs.

University of Maryland, University College, College Park, MD (Sept. 1995 to May 1998)
Part-time Instructor

University of Maryland, School of Business, College Park, MD (1996–1997)
Part-time Instructor

EDUCATION

Master's degree in Administrative Science (May 1984), Johns Hopkins University, Baltimore, MD.
Bachelor's degree in Computer Science (May 1975), Loyola College, Baltimore, MD.

Honors: Dean's List, graduation honors

PRESENTATIONS & PAPERS

Baker, John, *Cyber Security Education: Issues & Approaches,* Federal Information Systems Security Educators Association conference, March 10, 2004, College Park, MD

Baker, John, *Undergraduate Security Programs,* Infragard seminar, March 2, 2004, Johns Hopkins Applied Physics Lab, Laurel, MD.

Baker, John, *Developing Cyber Security Education Programs,* Society for Advanced Learning Technologies conference, Feb. 18, 2004, Orlando, FL.

Baker, John, *Ensuring Cyber Security, Security Education Programs,* CyberWatch Security Industry Group conference, Nov. 21, 2003, Greenbelt, MD.

Baker, John, *Information Literacy,* Society for Advanced Learning Technologies conference, July 27, 2001, College Park, MD.

July 20, 2004

The Honorable Sherwood Boehlert
Chairman, Science Committee
2320 Rayburn Office Building
Washington, DC 20515

Dear Congressman Boehlert:

Thank you for the invitation to testify before the U.S. House of Representatives Committee on Science on July 21, 2004, for the hearing entitled **Cyber Security Education: Meeting the Needs of Technology Workers and Employers**. In accordance with the Rules Governing Testimony, this letter serves as a formal notice of the federal funding I currently receive in support of my research.

I receive no federal funding directly supporting the subject matter on which I will testify, in either the current fiscal year or the two proceeding fiscal years.

Sincerely,

John Baker, Sr.
Director, Technology Programs
Division of Undergraduate Studies
School of Professional Studies
  In Business and Education
Johns Hopkins University

Chairman BOEHLERT. Thank you very much.
Mr. Spengler.

STATEMENT OF MR. ERICH J. SPENGLER, PRINCIPAL INVESTI-GATOR, ADVANCED TECHNOLOGY EDUCATION REGIONAL CENTER FOR THE ADVANCEMENT OF SYSTEMS SECURITY AND INFORMATION ASSURANCE, MORAINE VALLEY COMMU-NITY COLLEGE

Mr. SPENGLER. Good morning, Mr. Chairman and Members of the Committee. I would like to thank the Committee for the opportunity to comment on the role of community colleges in cyber security education.

Over the next few minutes, I will discuss how community colleges address the challenges in cyber security education and the ability of community colleges to focus on the practitioner skills necessary to adapt to the rapid changes in technology in the workplace.

Community colleges play a critical role in the education and training of our Nation's workforce. With an enrollment of 5.4 million credit students and five million non-credit students, these institutions train and educate 44 percent of our Nation's undergraduate students. A strength of community colleges is its flexibility of the curriculum, which is often designed specifically to train practitioners. This flexibility enables community colleges to respond quickly to changes in technology and the needs of business and industry. Community colleges facilitate career pathways from high schools to 2-year career programs and then additional pathways to 4-year colleges or universities. In addition, community colleges leverage the use of well-qualified adjunct and career faculty and also play a crucial role in the re-education and updating of the skills of current workers.

The NSF ATE Regional Center for Systems Security and Information Assurance and its partners recently conducted a survey of companies in five mid-western states to determine the job demand for IT security-related positions, desired skills, and preferred educational levels. A total of 340 responses were received. Respondents were divided into small, medium, and large companies. Ninety-nine percent of the respondents were concerned about Internet and computer security. Almost ¾ of respondents said their company currently employed people in IT security positions. Slightly more than half said there was a shortage in the current supply of qualified applicants for entry-level IT security positions.

There are significant opportunities for individuals who possess an Associate's degree, therefore, community colleges must continue to respond to growing industry demands for professionals possessing cyber security skills. Opportunity exists for Associate's degree graduates but also college pathways are important for those continuing education and careers.

Current strengths of community college cyber security programs include the utilization of the National Science Foundation ATE centers and resources. In addition, opportunities exist for community college faculty to participate in cyber security initiatives and information sharing with sponsored task groups, such as the FBI's InfraGard and the United States Secret Service Electronic Crimes Task Force.

Community colleges are also challenged to integrate security-related course work into existing IT programs and degrees. The

greatest challenge facing community colleges and their efforts to establish cyber security programs is faculty recruitment and development. The NSF ATE program currently provides vital resources for faculty development to enrich cyber security programs. For example, during the summer of 2004, the NSF ATE Regional Center for Systems Security and Information Assurance trained over 200 college faculty in security awareness, information assurance, network security, and wireless technologies.

Community colleges must also expand relationships with business and industry to develop innovative funding opportunities and partnerships. Partnering with national program models, such as the Cisco Systems Networking Academy, allows for greater implementation and consistency of curriculum.

The Center for System Security and Information Assurance is the first NSF ATE Regional Center for IT security. The center includes seven partner institutions representing five Midwest states. This center was established to address the needs for IT security professionals by increasing faculty expertise and higher education training programs in IT security and information assurance. This center collects, categorizes, adapts, enhances, standardizes, and evaluates curriculum and other training programs for community colleges and university faculty in students across the Midwest. The center partners with business and industry and local and federal agencies for program development.

To improve cyber security education and build the Nation's technical workforce, the Federal Government must continue to invest in the programs and the people that are making a difference in the education and training of our cyber security workforce. Without the support for programs such as the NSF Advanced Technological Education program, many institutions would not have the resources or faculty expertise to meet the challenges required to build quality cyber security programs.

This concludes my statement, Mr. Chairman and Members of the Committee. Thank you for allowing me to address the Committee on this issue.

[The prepared statement of Mr. Spengler follows:]

PREPARED STATEMENT OF ERICH J. SPENGLER

Good morning, Mr. Chairman and Members of the Committee. I would like to thank the Committee for the opportunity to comment on the role of community colleges in cyber security education. My name is Erich Spengler, and I am the Director and Principal Investigator for the National Science Foundation's ATE Regional Center for Systems Security and Information Assurance (CSSIA). I come to you with 16 years of combined experience in the classroom and the IT Industry. I am currently an Associate Professor in Computer Integrated Technology at Moraine Valley Community College in Palos Hills, Illinois.

- **What roles do community colleges play in the training of new workers and the retraining of current workers? What employment opportunities in cyber security are available for individuals with a certificate or a two-year degree?**

Role of Community Colleges

Community colleges play a critical role in the education and training the Nation's workforce. Some 1,173 community and technical colleges enroll 44 percent of all U.S. undergraduate students. The American Association of Community Colleges (AACC) notes that 200,000 certificates and 450,000 associate's degrees are granted each year. With an enrollment of 5.4 million credit students and five million non-credit

students, these institutions train and educate a significant percentage of the work-force.

One of the strengths of community colleges is the close relationship they maintain with local business and industry. This relationship may take many forms. For example, community college faculty are often asked to develop and deliver customized training solutions for business partners. Business partners play an important role in shaping career and technical programs by their participation as members of advisory committees. Another strength is the flexibility of the community college curriculum, which is often designed specifically to train practitioners. This flexibility enables community colleges to respond quickly to changes in technology. Community colleges also establish career pathways from high schools to two-year career programs and then additional pathways to four-year colleges or universities. This articulation of curriculum allows students to seamlessly continue higher levels of professional studies and education close to home.

Employment Opportunities

The NSF ATE Regional Center for Systems Security and Information Assurance (CSSIA) and its partners recently conducted a survey (http://www.cssia.org) of companies in five mid-western states to determine the job demand for IT security-related positions, desired skills, and preferred educational levels. I would like to share some of those results at this time.

- A total of 340 responses were received. Respondents were divided into small (less than 100 employees), medium (100–499) and large (500 or more) companies.
- An overwhelming 99 percent of respondents were concerned about Internet and computer security.
- Almost three-fourths of respondents said their company currently employed people in IT security positions.
- IT security positions were more likely to be part-time or shared positions (part-time security along with other IT duties) than dedicated (full-time IT security).

Table 1
Present/Projected Employment Needs for IT Security Positions

	Number Responding	Number of Openings	
		Dedicated Responsibility	Added Responsibility
Number of present openings	53	63	103
Number of projected openings within one year	60	96	141
Number of projected openings within three years	60	164	258

- Security responsibilities are being added to most IT professions, including network administrators, help desk specialists, network engineers, application developers, and systems analysts.
- Slightly more than half said there was a shortage in the current supply of qualified applicants for entry-level IT security positions.
- Large companies were more likely to be concerned about Internet and computer security and to have dedicated security positions.
- The most popular types of security training were self-study, commercial vendor training sites, and community college programs.

Table 2
Required Educational Level For An
Entry-Level IT Security Position
N=241

	Minimum	Preferred
None	7%	2%
High school diploma or GED	14%	1%
Certificate/licensure	15%	15%
Associate's degree	24%	13%
Bachelor's degree or higher	31%	62%
Other	9%	8%

- There are significant opportunities for individuals who possess an Associate's degree.
- Respondents indicated a significant number of current open IT security positions and projected even more openings over the next three years.

Community colleges must continue to respond to growing industry demands for professionals possessing cyber security skills. Although it is clear that there are career opportunities for professionals holding Associate's degrees, we must continue to develop pathways with four-year colleges and universities allowing those professionals to attain a higher level of education.

- **What are the current strengths and weaknesses of cyber security education and training programs? What "model" courses and programs currently exist? And what types of courses or programs need to be developed or more broadly implemented?**

Current strengths and weaknesses of cyber security education and training programs

Current strengths of cyber security education include the utilization of NSF ATE centers as resources for faculty development, internship programs and processes, dissemination and implementation of curriculum models, collaboration, and partnerships among academic institutions and business and industry. In addition, opportunities exist for community college faculty to participate in cyber security initiatives and information sharing with government-sponsored groups such as the FBI's InfraGard and the United States Secret Service Electronic Crimes Task Force.

However, much of the current cyber security curriculum typically focuses on networking-related technologies. There is a need to expand the emphasis beyond networking to serve the greater spectrum of IT curriculum. Specialties might included forensics, programming and secure coding, information assurance, and e-commerce and secure communications.

Community colleges are also challenged to integrate security-related coursework into existing IT programs and degrees. Three career areas must be addressed: (1) the focused cyber security practitioner specializing in their field of study, (2) the IT professional not dedicated to security but who is charged with the protection of critical information and infrastructure, and (3) non-IT-related professionals such as health care personnel.

Model courses and programs

As cyber security technology emerges so must the programs within the community colleges. There is debate regarding modeling of curriculum on industry certification. This debate centers on the delicate balance between certification preparation and required skill sets. Certifications provide a reasonable direction and solid groundwork representing industry needs. However, barriers exist for standardized academic models that reflect the skills defined by these industry certifications: (1) security-related industry certifications continue to proliferate, making it difficult to identify which certifications would provide the best models, and (2) skills outlined in industry certification often require costly effort to be implemented into an academic framework.

Community colleges have identified four approaches to developing and offering courses and programs: (1) four-semester programs of study leading to Associate's degrees, (2) two-semester programs leading to institution-conferred certificates, (3)

credit courses that are part of an existing program of study, and (4) non-credit programs of preparation for industry certification.

The NSF ATE Regional Center for Systems Security and Information Assurance (CSSIA) is developing an adoptable model that reflects both industry certifications and practitioners' required skills. The CSSIA center is working within each of the partner states to establish model four-semester and certificate programs that reflect current and relevant industry certifications and skills.

Development of programs

Collaboration among community colleges to reduce duplication of efforts is still needed. The establishment of cyber security programs can be expensive and require a prolonged development cycle. Additionally, we should consider the importance of the adaptation and dissemination of instructional materials and best practices. As an example, to help reduce implementation costs of quality learning environments, the NSF ATE CSSIA center developed an innovative use of laboratory equipment through remote access and management. Additionally, partnering with national program models, such as the Cisco Systems Networking Academy, allows for greater implementation and consistency of curriculum.

- **What are the challenges you face in recruiting and training cyber security faculty? What type of programs or opportunities do you provide to help keep faculty current?**

Challenges in recruiting and training cyber security faculty

The greatest challenge facing community colleges and their efforts to establish cyber security programs is faculty recruitment and development. Community colleges must try to compete with business and industry for skilled practitioners. An additional challenge occurs when individuals interested in becoming faculty members possess the necessary technological skills, but lack teaching experience.

Programs or opportunities to help keep faculty current

In 2002, the American Association of Community Colleges (AACC) sponsored the AACC/NSF Cyber Security Workshop. The workshop served as a catalyst for community college professionals interested in cyber security by identifying workforce and curricular needs and by establishing a forum for collaboration among community colleges.

The NSF ATE program has provided vital resources to a number of community colleges in an effort to establish cyber security programs. These projects allocate a significant portion of the funding for faculty development. The funds can be used in activities such as product training, professional externship opportunities, and graduate-level courses and workshops.

During the summer of 2004, the NSF ATE Regional Center for Systems Security and Information Assurance (CSSIA) trained over 200 college faculty in Security Awareness, Information Assurance, Network Security, and Wireless technologies. CSSIA will continue to provide training opportunities in new and emerging skills for faculty in subsequent years.

It is clearly our belief that without these training programs, the cyber security initiatives available to attending faculty would not move forward to meet growing industry practitioner demands. Another model designed to keep faculty current in emerging IT skills is the Working Connections Faculty Development Institute. Working Connections is co-sponsored by the NSF ATE National Workforce Center for Emerging Technologies (NWCET), AACC and Microsoft Corporation to develop professional skills of faculty in several regions throughout the U.S.

- **What can the Federal Government do to improve cyber security education and build the Nation's technical workforce?**

First, the Federal Government can encourage government agencies to provide to community colleges their job descriptions and titles that are appropriate for cyber security graduates of two-year community and technical college programs.

Next, to improve cyber security education and build the Nation's technical workforce, the Federal Government must continue to invest in the programs and people that are making a difference in the education and training of our cyber security workforce. Without the support from programs such as the NSF Advanced Technological Education (ATE) Program, many institutions would not have the resources or faculty expertise to meet the challenges required to build quality cyber security programs.

This concludes my statement Mr. Chairman and Members of the Committee. Thank you for allowing me to address the Committee on this issue.

BIOGRAPHY FOR ERICH J. SPENGLER

Director/PI—CSSIA, NSF Regional Center for Systems Security and Information Assurance

Erich Spengler holds a Master's degree from Loyola University and has been a full-time faculty member at Moraine Valley Community College for the past nine years. Mr. Spengler also has an extensive background in information technology, security and information assurance. He holds several major industry certifications, including CISSP, MCSE and CCNP. Additionally, he has a broad background in network design and infrastructure implementation.

Mr. Spengler currently serves as the Director and Principle Investigator for the National Science Foundation (NSF) ATE Regional Center for Systems Security and Information Assurance (CSSIA). This regional center serves a five-state area of the Midwest and focuses on a field which is critical to homeland security and which has a large demand for qualified workers. The center is collecting, adapting, and enhancing curricula in cyber security, modeling certificate and degree programs, and providing professional development for college faculty in the region.
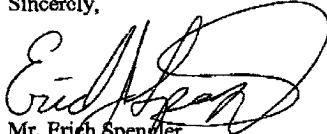
7/19/2004

The Honorable Sherwood Boehlert
Chairman, Science Committee
2320 Rayburn Office Building
Washington, DC 20515

Dear Congressman Boehlert:

Thank you for the invitation to testify before the U.S. House of Representatives Committee on Science on **"Cybersecurity Education – Meeting the Needs of Technology Workers and Employers"** on Wednesday, July 21, 2004. In accordance with the Rules Governing Testimony, this letter serves as formal notice of the federal funding to my college.

- Amount: 2,997,615.
- Grant Number: 0302612
- Federal Agency/Source Title: National Science Foundation: NSF Advanced Technological Education (ATE)
- Fiscal Year Received: September 1, 2003

Sincerely,

Mr. Erich Spengler
Principal Investigator
Center for the Advancement of Systems Security
& Information Assurance
Moraine Valley Community College
10900 South 88th Avenue
Palos Hills, IL 60465-2175

Chairman BOEHLERT. Thank you, Mr. Spengler. And I can't help but observe that 22 years ago, when I was a freshman sitting down on the first row at the very end, community colleges weren't even on the radar screen of the National Science Foundation. And since then, I have worked very hard, joined by colleagues, Republicans and Democrats alike, to make certain the great opportunities presented by community colleges have been recognized by the National Science Foundation. And so, in the late '80's was born the ATE program, the Advanced Technological Education program. And now, NSF recognizes what you know very well, that the community colleges are very important in the educational process of America. So thank you for what you are doing so much.

Lieutenant Aparicio.

STATEMENT OF SECOND LIEUTENANT DAVID J. APARICIO, DEVELOPMENTAL ELECTRICAL ENGINEER, INFORMATION DIRECTORATE, AIR FORCE RESEARCH LABORATORY

Second Lieutenant APARICIO. Yes, sir.

Mr. Chairman, Congressman Gordon, Members of the Committee, and staff, I very much appreciate the opportunity to provide testimony in my personal capacity on cyber security education, in particular my experience in the Advanced Course in Engineering on Cyber Security.

And as an introduction on the National Strategy to Secure Cyberspace, President George W. Bush wrote that "securing cyberspace is an extraordinarily difficult strategic challenge that requires coordinated and focused effort from our entire society" and "the cornerstone of America's cyberspace security strategy is a public-private partnership."

Last summer, I had the distinct privilege in participating in the Advanced Course in Engineering, or ACE, on Cyber Security at the Air Force Research Laboratory Information Directorate in Rome, New York. The program immersed me in 10 grueling weeks of research, problem solving, and report writing on a variety of cyber security issues. I completed all requirements to call myself an ACE graduate and earned the distinction of Class Valedictorian. I gained far more than just a certificate of completion. I gained a mastery of the issues on cyber security, which challenge our Nation today and shape our future.

ACE uses a unique approach toward running the program. Once a week, students are immersed in a one-day lecture covering a specific area in cyber security, concluding with an assignment of a real-world problem. Students must solve the problem, write a report detailing their solution. For the rest of the week, students work with their personal mentors on military and industry projects with the Rome Research Site. This unique combination of high-intensity instruction and military and industry projects creates an environment that develops cyber security leadership and situational awareness vital for our future. ACE taught me not only technical confidence but mental flexibility to solve any problem placed in front of me, academic or critical.

I proceeded with great enthusiasm and duty because cyber security is a gravely serious business. ACE introduced me to many of the challenges of cyber security. Responding to the challenges, I re-

quested to return to the Air Force Research Laboratory Information Directorate to contribute to the defense of our Nation through cyber security awareness. With my new view on the world, I plan to eventually work for the Central Intelligence Agency or the National Security Agency.

The Advance Course in Engineering on Cyber Security addresses the challenge of the National Strategy to Secure Cyberspace by developing the top students in pre-commissioning officer training programs into the next generation of cyber security leaders. Through public and private partnerships among the Air Force Research Laboratory Information Directorate, Syracuse University, the Computer Applications and Software Engineering Center of the New York State Office of Science, Technology, and Academic Research, the Griffiss Institute on Information Assurance, and several corporations, the ACE follows the proven model of the General Electric Edison course to transform engineers into original thinkers, problem solvers, and technical leaders.

Far from creating another computer security training program, the ACE seeks to develop cyber security leaders through intensive, formal education, teamwork, problem solving, mentoring, and immersion into a work environment. Gene Kranz best described his mindset of an engineering leader in his book "Failure Is Not an Option: Mission Control from Mercury to Apollo 13 and Beyond." As director of the National Aeronautics and Space Administration's mission control in the Apollo era, Kranz led his engineers into uncharted territory, the moon, and established our unchallenged leadership of space.

Cyberspace in the 21st century is no less challenging than outer space in the 20th century. Besides, the security of our Nation relies on establishing and maintaining unchallenged leadership in cyberspace.

In two years at the Rome Research Site, ACE has attracted students from 25 colleges in 17 states. In addition to Reserve Officers' Training Corps, or ROTC, the students include National Science Foundation fellows, Junior ROTC cadets, and civilian scientists and engineers committed to careers in cyber security. Educators include faculty from Syracuse University, the U.S. Military Academy at West Point, and the State University of New York, in addition to domain experts from the Air Force Research Laboratory and industry.

The Federal Government can help cyber security education in two ways. First, the government could increase efforts to recruit younger generations, namely middle school and high school students. ACE currently reaches to junior ROTC programs to train college-bound students in cyber security. Secondly, the government should consider increasing its cyber security education through public service announcements. Just as the government shows anti-drug campaign videos on television, basic cyber security videos should be a staple of the American television.

Mr. Chairman, Members of the Committee, and staff, thank you again for this opportunity to present testimony and thank you for your continuing support of the Air Force cyber security education efforts.

[The prepared statement of Second Lieutenant Aparicio follows:]

45

PREPARED STATEMENT OF SECOND LIEUTENANT DAVID J. APARICIO

Mr. Chairman, Members of the Committee, and Staff, I very much appreciate the opportunity to provide testimony in my personal capacity on cyber security education and, in particular, my experience in the Advanced Course in Engineering (ACE) on Cyber Security. In his introduction of *The National Strategy to Secure Cyberspace,* President George W. Bush wrote that "securing cyberspace is an extraordinarily difficult strategic challenge that requires coordinated and focused effort from our entire society" and that "the cornerstone of America's cyberspace security strategy is a public-private partnership."

Last summer, I had the distinct privilege of participating in the Advanced Course in Engineering (ACE) on Cyber Security at the Air Force Research Laboratory Information Directorate in Rome, New York. The program immersed me into ten grueling weeks of research, problem solving, and report writing on a variety of cyber security issues. I completed all requirements to call myself an ACE graduate and I earned the distinction of Class Valedictorian. I gained far more than just a certificate of completion. I gained a mastery of the issues of cyber security, which challenge our nation today and shape our future.

ACE uses a unique approach towards running the program. Once a week, students are immersed into one-day lecture covering a specific area in cyber security, concluding with the assignment of a real-world problem. The students must solve the problem and write a report detailing their solution. For the rest of each week, students work with personal mentors on military and industry projects within the Rome Research Site. This unique combination of high-intensity instruction and military and industry projects creates an environment that develops cyber security leadership and situational awareness vital to our future. ACE taught me not only technical competence, but mental flexibility to solve any problem placed in front of me—academic or critical.

I proceeded with great enthusiasm and duty because cyber security is a gravely serious business. ACE introduced me to many of the challenges of cyber security. Responding to the challenge, I requested to return to the Air Force Research Laboratory Information Directorate to contribute to the defense of our nation through cyber security awareness. I plan to eventually work for the Central Intelligence Agency or the National Security Agency with my new view of the world.

Many of my fellow ACE graduates received commissions where they put to good use their increased command of cyber security and their appreciation of its impact of national security.

ACE BACKGROUND

The Advanced Course in Engineering (ACE) on Cyber Security addresses the challenge of *The National Strategy to Secure Cyberspace* by developing the top students in pre-commissioning officers training programs into the next generation of cyber security leaders. Through a public-private partnership among the Air Force Research Laboratory Information Directorate, Syracuse University, the Computer Applications and Software Engineering (CASE) Center of the New York State Office of Science, Technology, and Academic Research, the Griffiss Institute on Information Assurance, and several corporations, the ACE follows the proven model of the General Electric Edison course to transform engineers into original thinkers, problem solvers, and technical leaders.

Far from creating another computer security training program, the ACE seeks to develop cyber security leaders by drawing from the top students in Air Force, Army, and Navy pre-commissioning training programs, in addition to the best among our civilian college students. The pedagogical philosophy underlying the ACE seeks to develop leadership skills through intensive formal education, teamwork, problem solving, mentoring, and immersion in a work environment.

The ACE philosophy is best summarized in the following paradigm: faced with a real-world problem, the graduates of the ACE learn to:

1. formulate a clear problem statement,
2. make reasonable assumptions,
3. apply sound analytical techniques and engineering tools,
4. solve the problem to a certain depth,
5. perform risk analysis on the solution, and
6. deliver a solution on time through effective communication means.

Gene Kranz best described this mindset of an engineering leader in his book "Failure Is Not an Option: Mission Control from Mercury to Apollo 13 and Beyond." As director of the National Aeronautical and Space Administration's mission control

in the Apollo era, Kranz led his engineers into uncharted territory—the Moon—and established our unchallenged leadership of space.

Cyberspace in the twenty-first century is no less challenging than outer space in the twentieth century. Besides, the security of our nation relies on establishing and maintaining unchallenged leadership in cyberspace.

In its second year at the Rome Research Site, the ACE has attracted 26 students from 25 colleges in 17 states. In addition to Reserve Officers' Training Corps (ROTC), the students include fellowship recipients from the National Science Foundation Scholarship for Service Cyber Corps program, cadets from the Air Force Junior ROTC, and civilian scientists and engineers committed to careers in cyber security.

The educators include faculty from Syracuse University, the United States Military Academy at West Point, and the State University of New York, in addition to domain experts from the Air Force Research Laboratory and industry.

Besides attending formal classes and solving real-world problems, the students spend about three days each week working under the tutelage of a mentor. The mentors include active duty and retired officers at the Air National Guard North East Air Defense Sector, the Air Force Research Laboratory, and several local companies.

The duration of the ACE is ten weeks during the June-August timeframe. Each week focuses on one area of cyber security as detailed below:

1. Legal Issues: Internet laws and cyber crime; the Fourth Amendment of the United States Constitution; search and seizure of data; rights and privacy issues; government versus private workplace; search warrants and wiretap laws; and the Patriot Act.

2. Security Policies: Establishing and implementing security policies; confidentiality, integrity, and availability considerations; identifying vulnerabilities and threats; and establishing disaster response and recovery procedures.

3. Cryptography: Mathematical basis for data encryption; substitution ciphers and the Data Encryption Standard; private-key and public-key cryptography; key distribution and trusted authority; and digital signatures.

4. Computer Security: Operating systems and file system security; passwords and one-way hashes; user-space administration; archiving and back-up strategy; intrusion detection; and disaster response and recovery.

5. Digital Forensics: Procuring and analyzing digital evidence; preserving the chain of custody of digital evidence; recovering hidden data on hard drives; classifying file systems; analyzing slack and sector data; and recovering lost clusters.

6. Network Security: Internet protocol format and vulnerabilities; protocol and implementation flaws; buffer overflow; denial-of-service attacks; distributed attacks; e-mail; domain name system; and web servers.

7. Network Defense: Host and network security; firewalls and periphery intrusion detection systems; bastion hosts; network monitors and traffic analyzers; network logfiles; detecting anomalous behavior; and network recovery.

8. Network Attack: Port scanners and packet sniffers; IP spoofing; identifying vulnerabilities; designing and implementing network attacks; engineering malicious code; worms and viruses; and offensive cyber warfare.

9. Steganography: Data hiding in images; classifying steganography algorithms and tools; categorizing vessel capacity; detection and recovery of hidden data; digital watermarking; streaming media steganography; and multilingual steganography.

10. Next Generation Cyber Security: Wireless local area networks; wireless encryption protocols; Next Generation Internet Protocols; embedded systems; and third generation (3G) cell phones and personal data assistants.

For each topic, the instructor in charge assigns a substantial real-world problem that requires 40 to 80 hours of teamwork to solve. Students work on teams of three to solve each problem, then write and submit individual reports.

RECOMMENDATIONS

The Federal Government can help cyber security in two ways. First, the government could increase efforts to recruit the younger generations—namely middle and high school students. ACE currently reaches out to junior ROTC programs to train college-bound students in cyber security. Secondly, the government should consider increasing its cyber security awareness through public service announcements. Just

as the government shows anti-drug campaign videos on television, basic cyber security videos should be a staple of American television.

BIOGRAPHY FOR SECOND LIEUTENANT DAVID J. APARICIO

2Lt David Aparicio is a developmental electrical engineer for the Air Force Research Laboratory Information Directorate in Rome, New York. He supports research and development of tools for multi-sensor exploitation and communications intelligence. Lt. Aparicio was born in Portland, Oregon, but calls Sugar Land, Texas, his native home. He earned his Bachelor of Science degree in electrical and computer engineering at Baylor University and received his commission as a Blue Chip graduate of Baylor's ROTC program in 2003. Lt. Aparicio was also a graduate and the valedictorian of the Advanced Course in Engineer on Cyber Security in 2003. In his free time, Lt. Aparicio enjoys photography, writing, and playing soccer.
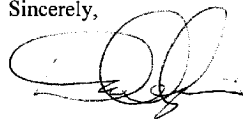
21 July 2004

The Honorable Sherwood Boehlert
Chairman, Science Committee
2320 Rayburn Office Building
Washington, DC 20515

Dear Congressman Boehlert:

Thank you for the invitation to testify before the U.S. House of Representatives Committee on Science on July 21st for the hearing entitled *Cybersecurity Education – Meeting the Needs of Technology Workers and Employers*. In accordance with the Rules Governing Testimony, this letter serves as formal notice of the federal funding I receive.

I received no federal funding directly supporting the subject matter on which I testified, in the current fiscal year or either of the two proceeding fiscal years.

Sincerely,

David Aparicio, 2LT, USAF

Chairman BOEHLERT. Thank you very much, Lieutenant, and thank you for calling me "sir." I was a Specialist 3rd Class, and so when an officer calls me "sir," it sort of puffs me up a little bit.
How many were in your class?
Second Lieutenant APARICIO. My class? There were 14.
Chairman BOEHLERT. And I think this year's boot camp has 28, double the number, something like that.
Second Lieutenant APARICIO. I will have to get back to you on the exact number.

Chairman BOEHLERT. Well, the doctor is right behind you nodding his head yes, so I have the privilege of addressing him. It is exciting to think about your future.

Second Lieutenant APARICIO. Thank you.

Chairman BOEHLERT. Ms. Rogers.

STATEMENT OF MS. SYDNEY ROGERS, PRINCIPAL INVESTIGATOR, ADVANCED TECHNOLOGY EDUCATION REGIONAL CENTER FOR INFORMATION TECHNOLOGY, NASHVILLE STATE COMMUNITY COLLEGE

Ms. ROGERS. Good morning, Mr. Chairman, and Representative Gordon, and Members of the Committee.

[Slide.]

Today we examine the challenge of educating skilled workers within the context of a world that is vastly different from the world when I began my career 30 years ago. My colleagues and I believe it is important to understand this new context in order to adequately understand what is needed to design and implement education programs that will develop a world-class competitive workforce with respect to cyber security.

[Slide.]

The context of today's educational programs involves new and constantly evolving technologies that are dramatically changing every aspect of our society. New threats, such as terrorism and identity theft, pose even greater security challenges while the distributed nature of systems and data storage complicates the control of security exponentially.

[Slide.]

Our response from a technical perspective has been to mitigate these exposures as much as possible through techniques, such as patches and virus protection software, and then reduce the exposure to risk with technologies like firewall protection and encryption. As a result, we find ourselves addressing the symptoms and not the real problem: systems designed and built without consideration of security. Technicians work on individual problems without an overall context. One Chief Network Officer in Nashville explains it this way: "We are fixing the symptoms because we are dealing with legacy systems and our only solution is to fix the symptom."

[Slide.]

Education's response today is to focus technician education on training for specific technical skills through certification programs, expansion of course content, addition of new courses, new concentrations, and new two- and four-year degrees, and this slide shows in the background some of the programs we are doing at my college and others in Tennessee.

[Slide.]

All of these approaches are necessary in order to protect today's systems, but how do we educate for tomorrow's cyber risk? How do we build a workforce that will know how to use what they know in context and that will have the skills necessary to understand constantly changing technologies and what is needed to both use them and protect them?

[Slide.]

Our industry partners in Tennessee tell us, as depicted here, cyber security professionals, who require the most extensive technical knowledge, also represent a relatively small number of workers who need specific highly technical cyber security skills. To be sure, all information technology professionals must possess technical skills necessary to develop and maintain secure systems. Our employers tell us that all workers need some understanding of cyber security and some level of expertise in these skills. Even though community colleges and our NSF work at my center touch all three of these areas, our ATE focuses on the preparation of IT professionals.

[Slide.]

To meet today's need and, at the same time, build a workforce that meets tomorrow's needs, we must move beyond traditional curriculum development methods that focus on silos of content with little context. That is not the first time—you have already heard that today. We need to develop teaching and learning methods that foster learning, thinking, and problem solving in the context of the real world.

[Slide.]

We have developed model programs for bringing these workplace experiences directly to the students and creating more adaptable workers. Our contextual and problem-based methods all share some common characteristics. First, they are all based on authentic workplace problems. To bring these authentic workplace problems into the classroom requires a close and consistent working relationship with our business and industry partners. Just as technology in the workplace is changing constantly, these authentic experiences must also change. By implementing these experiences for students, we are also building a curriculum that adapts and changes with changing technology and situations. Using these methods, then, we can create an educational system that builds a closer link between the content taught and the actual workplace application while also developing workers who are more able to adapt the knowledge they have to a rapidly changing world. Finally, to effectively teach using these methods, faculty must learn to function as highly skilled facilitators who guide students to discover and understand the appropriate scientific and technical knowledge.

[Slide.]

In Tennessee, the NSF/ATE projects have helped to develop a strong foundation for re-educating current workers and building programs for the future. For instance, we have just initiated a program with the Tennessee Telecommunications Association to re-educate some of their workers. Our faculty would not have the skills and knowledge necessary to do this program properly if we had not had the funding from the ATE program to provide faculty development opportunities for them.

As for the future workforce in IT, we have piloted an exciting program that brings real-time industry technical problems directly to the classroom to be solved by students by partnering industry technicians with faculty at the community colleges and universities. Last year, some of these problems included a network security problem at a music company and a distributed data and net-

working problem for the Saturn Corporation. Students at Nashville State Community College, Roane State Community College, Tennessee State University, Middle Tennessee State University, and Austin Peay State University participated in this program to work more closely with business and industry.

[Slide.]

The concepts and projects I have highlighted have given us a fundamental knowledge base for educating cyber security workers as well as all workers who need to understand their work within the context of needed security. The road that has brought us to this point required several years of work in faculty development, materials development, and building partnerships with business and industry. Others around the country have worked on similar concepts with slightly different approaches. Together, and with the support of the NSF/ATE program, in two weeks, we will convene more than 250 community college technological faculty and administrators, along with some of their industry partners, university partners, and secondary partners in 31 teams from 17 states across the country in Nashville for Synergy 2004. The teams are represented on the map you see. At Synergy, these teams will begin to develop plans for educational reform of IT and IT-enabled programs in their own regions of the country. Their work will be anchored by presentations from leading experts in teaching and learning, such as John Bransford, Jay McTighe, and Pam Tate. To provide the context and one global perspective, Doug Busch, the Chief Information Officer for Intel, will talk to us about the type of IT workforce we need to build if the country is to be competitive and to create jobs that will not be candidates to offshoring. I expect Mr. Busch to confirm that we are on the right track with the reform programs we have stated. In an interview Mr. Busch recently provided for us, he states, "One of the key problems we see as private sector participants trying to contribute to improved technological education is the lack of a central focus for U.S. education. Reform of technical education is so fragmented in the United States that it often seems impossible to have a significant positive impact. This is very different from the situation in the countries the United States competes with. I believe it would be very useful to have a single focus point."

[Slide.]

We also expect those who attend Synergy to leave motivated and prepared to begin to implement meaningful change. They will need to be supported in their efforts, and I believe the ATE program is looking for ways to do that. As I have explained, to be successful, these community colleges will need to be closely aligned with their business, industry, and government employers who will rely on the future workforce. Although our program and others have been successful in partnering with business and industry, doing so remains a barrier to many programs. Therefore, government programs that provide incentives for business and industry participation with community colleges would benefit all concerned. Initiatives that provide opportunities for faculty and students to participate in real-world internships will further support these efforts. Also, the educational infrastructure in this country as it is currently structured creates silos of educational programs. To make real and sub-

stantial progress, we will need incentives to break down these bar-
riers so that we can begin to build an education system for the fu-
ture, one in which cyber security is a fundamental part of the con-
text and the outcome.

And the government's continued support of the ATE program so
that the necessary materials development, faculty development in
teaching and learning, and up-to-date technical knowledge can
occur will be vital to the success of these colleges. Finally, to
achieve the best result, technological education should be made a
national priority.

Thank you for this opportunity.

[The prepared statement of Ms. Rogers follows:]

PREPARED STATEMENT OF SYDNEY ROGERS

Good morning Mr. Chairman and Members of the Committee. My name is Sydney
Rogers and I am Vice President of Community and Economic Development at Nash-
ville State Technical Community College (NSCC) in Tennessee. NSCC is located in
an urban area and serves a student body of approximately 7000 racially diverse stu-
dents including approximately 26 percent African American. The average age of an
NSCC student is 30 years. Many of our current students are already in the work-
force and attend NSCC to acquire new work skills, some enter the workforce di-
rectly or transfer to Tennessee State University, a Historically Black College or Uni-
versity (HBCU) located less than five miles from our campus. Many others transfer
to Middle Tennessee State University (MTSU) in Murfreesboro, Tn., or Austin Peay
State University (APSU) in Clarksville, Tn.

For nearly a decade, Nashville State Community College has led a regional effort
to transform Information Technology education. The Advanced Technological Edu-
cation (ATE) program of the National Science Foundation (NSF) has funded these
activities. Our partners include the regional universities just listed above, local
school systems, and dozens of business partners such as Saturn, BMI, Dell Com-
puter, EDS, Hospital Corporation of America (HCA), and Vanderbilt University
Medical Center, among others.

Today we examine the challenge of educating skilled workers within the context
of a world that is vastly different from the world when I began my career 30 years
ago. My colleagues and I believe it is important to understand this new context in
order to adequately understand what is needed to design and implement education
programs that will develop a world-class competitive workforce, with respect to
cyber security.

The context of today's educational programs involves new and constantly evolving
technologies that are dramatically changing every aspect of our society. New
threats, such as terrorism and identity theft pose even greater security challenges
while the distributed nature of systems and data storage complicates the control of
security exponentially.

Our response from a technical perspective has been to mitigate these exposures
as much as possible through techniques such as patches and virus protection soft-
ware and then reduce the exposure to risk with technologies like firewall protection
and encryption. As a result, we find ourselves addressing the symptoms and not the
real problem; systems designed and built without consideration of security. Techni-
cians work on individual problems without an overall context. One Chief Network
Officer in Nashville explains it this way, "We are fixing the symptoms because we
are dealing with legacy systems and our only solution is to fix the symptom."

Education's response today is to focus technician education on training for specific
technical skills through certification programs, expansion of course content, addition
of new courses, new concentrations, and new two- and four-year degrees and this
slide shows some of the programs we are doing at my college and others in Ten-
nessee. All of these approaches are necessary in order to protect today's systems,
but how do we educate today for tomorrow's cyber risk? How do we build a work-
force that will know how to use what they know in context and that will have the
skills necessary to understand constantly changing technologies and what is needed
to both use and protect them?

Our industry partners in Tennessee tell us, as depicted here; cyber security pro-
fessionals who require the most extensive technical knowledge also represent a rel-
atively small number of workers who need specific highly technical cyber security
skills. To be sure, all information technology professionals must possess the tech-

nical skills necessary to develop and maintain secure systems. Our employers tell us that all workers need some understanding of cyber security and some level of expertise in these skills. Even though community colleges and our NSF work touch all three of these areas, our ATE focus is in the preparation of IT professionals.

To meet today's need and at the same time build a workforce that meets tomorrow's needs, we must move beyond traditional curriculum development methods that focus on silos of content with little context. We need to develop teaching and learning methods that foster learning, thinking, and problem solving in the context of the real world. Not only do workers need to know how to use their knowledge "in context," but educational research has shown us that such methods produce great improvements in learning and that students prepared in this way more easily transfer what they know to new and different situations. My colleagues and I believe the ability to transfer knowledge more quickly will result in more adaptable workers who will be able to understand more quickly and apply changing technologies. The term the researchers use for this is "adaptive expertise." Through a previous NSF/ATE grant called (SEATEC–DUE 9850307), NSCC in conjunction with Saleh Sbenaty of Middle Tennessee State University (MTSU), conducted a research study that tested the theory that students would more easily transfer technical knowledge learned using problem based case studies than they would knowledge learned using traditional methods. Although we did not address cyber security directly in this study, we believe the concept of knowledge transfer is important in building a workforce that is cyber security competent. For more information about this study and the results please see the article by Dr. Saleh Sbenaty of MTSU in the Proceeding of the 2002 American Society of Engineering Education (ASEE) Annual Conference and Exposition. The community colleges in Tennessee have learned much about how to transfer this research in to practice through our NSF/ATE grants. In 1998, Gerhard Salinger one of the lead program officers of the ATE program introduced us to John Bransford from Vanderbilt University (now at University of Washington). Dr. Bransford is the one of the editors of the National Research Council's publication "How People Learn," an extensive collection of recent research on the subject. Working with him and his team of researchers, we have begun to transform the way we structure the learning environment. For information on how we have used this research to transform teaching and learning, see article in American Association of Community College Journal, October/November 2003 "Transferring Teaching and Learning Research to the Classroom" by Sydney Rogers and George Van Allen.

We have developed model programs for bringing these workplace experiences directly to the students and creating more adaptable workers. Our contextual and problem-based methods all share some common characteristics. First, they are all based on authentic workplace problems. To bring these authentic workplace problems into the classroom requires a close and consistent working relationship with our business and industry partners. Just as technology and the workplace are changing constantly, these authentic experiences must also change. By implementing these experiences for students we are also building a curriculum that adapts and changes with changing technology and situations. Using these methods, then, we can create an educational system that builds a closer link between the content taught and the actual workplace application while also developing workers who are more able to adapt the knowledge they have to a rapidly changing world. Finally, to effectively teach using these methods, faculty must learn to function as highly skilled facilitators who guide students to discover and understand the appropriate scientific and technical knowledge. *(See our websites for case studies of some of these authentic problems. www.cite-tn.org and www.casefiles.org)*

In Tennessee, the NSF/ATE projects have helped to develop a strong foundation for reeducating current workers and building programs for the future. For instance, we have just initiated a program with the Tennessee Telecommunications Association (TTA) to re-educate some of their workers. In a series of courses, including two courses on network security, our community college faculty will teach the TTA employees using the contextual and problem-based methods in the form of problem-based case studies and real-time problems. Our faculty would not have the skills and knowledge to do this if we had not had the funding from the ATE program to provide faculty development opportunities for them. Our NSF/ATE Center for Information Technology (CITE) sponsors an electronic marketplace for workforce development called the Tennessee IT Exchange. Employers and students can find out where to obtain education on the latest technologies, including cyber security. The community colleges in the region, Nashville State, Columbia State, and Roane State along with the regional universities, TSU, MTSU, and APSU, all contribute to the Exchange. The Tennessee IT Exchange may be viewed at *www.cite-tn.org*. CITE also

53

partnered with the local workforce investment board to H1B–Visa funds to middle Tennessee for retraining in IT. A portion of this training will be on cyber security.

As for the future workforce in IT, we have piloted an exciting program that brings real-time industry technical problems directly into the classroom to be solved by students by partnering industry technicians with faculty at the community colleges and universities. Last year, some of these problems included a network security problem at a music company and a distributed data and networking problem for the Saturn Corporation. Results at both the community college and the university have exceeded expectations. For instance, Saturn and EDS worked with us on two problems, one at NSCC and one at Tennessee State University. Evaluations from students, faculty, and employers tell us that students are more engaged and learn better and Saturn is now considering implementing some of the student solutions at the plant. See attached description of this type problem solved by students at the DOE Y12 Security Complex in Oak Ridge, TN.

Last year and this year, CITE partnered with the Nashville Technology Council to sponsor faculty and student teams at the Technology Council's annual "IT Security Conference." At this conference, students' interaction with security experts and vendors provides a context for their learning. CITE is also helping to establish "IT Academies" in high schools across Tennessee to build a pipeline of students who will enter the workforce or college in technical IT careers. One such academy is located at Stratford High School, an inner city, mostly minority school in Nashville. It opened in the fall of 2003 with 97 students and nine faculty members. Thus far, 57 additional students have applied to attend in the fall of 2004.

The concepts and projects I have highlighted have given us a fundamental knowledge base for educating cyber security workers as well as all workers who need to understand their work within the context of the needed security. The road that has brought us to this point required several years of work in faculty development, materials development, and building partnerships with business and industry. Others around the country have worked on similar concepts with slightly different approaches. Together and with the support of the NSF/ATE program, in two weeks we will convene more than 250 community college technological faculty and administrators, along with some of their industry partners, university partners, and secondary school partners in 31 teams from 17 states across the country in Nashville for "Synergy 2004" *(DUE 0412846)*. At "Synergy," these teams will begin to develop plans for educational reform of IT and IT enabled programs in their own regions of the country. Their work will be anchored by presentations from leading experts in teaching and learning such as John Bransford, Jay McTighe, and Pam Tate. To provide the context and one global perspective, Doug Busch, the Chief Information Officer for Intel, will talk to us about the type of IT workforce we need to build if the country is to be competitive and to create jobs that will not be candidates to offshore. I expect Mr. Busch to confirm that we are on the right track with the reform programs we have started. In an interview Mr. Busch recently provided for us, he states, "One of the key problems we see as private sector participants trying to contribute to improved education is the lack of a central focus for U.S. education. Reform of technical education is so fragmented in the United States that it often seems impossible to have a significant positive impact. This is very different from the situation in the countries the United States competes with. I believe it would be very useful to have a single focus point." Several colleges and universities around the country have collaborated to produce "Synergy." They are Nashville State Technical Community College in Nashville Tennessee, University of Arkansas at Fort Smith, University of Massachusetts in Boston Massachusetts, Springfield Technical Community College in Springfield Massachusetts, and Bellevue Community College in Bellevue Washington. Please see *www.synergy2004.org* for a complete description of the meeting.

We also expect those who attend "Synergy" to leave motivated and prepared to begin to implement meaningful change. They will need to be supported in their efforts and I believe ATE program is looking for ways to do that. As I have explained, to be successful, these community colleges will need to be closely aligned with their business, industry, and government employers who will rely on the future workforce. Although our program and others have been successful in partnering with business and industry, doing so remains a barrier to many programs. Many small businesses cannot donate the needed time and resources to our efforts. Therefore, government programs that provide incentives for business and industry participation with community colleges would benefit all concerned. Too, initiatives that provide opportunities for faculty and students to participate in real-world internships will further support these efforts. Also, the educational infrastructure in this country as it is currently structured creates "silos" of educational programs. To make real and substantial progress, we will need incentives to break down these barriers

so that we can begin to build and education system for the future; one in which cyber security is a fundamental part of the context and the outcome.

And, the government's continued support of the ATE program so that the necessary materials development, faculty development in teaching and learning, and up-to-date technical knowledge can occur will be vital to the success of these colleges. Finally, to achieve the best result, technological education should be made a national priority.

Thank you for the opportunity to give you this information about our programs.
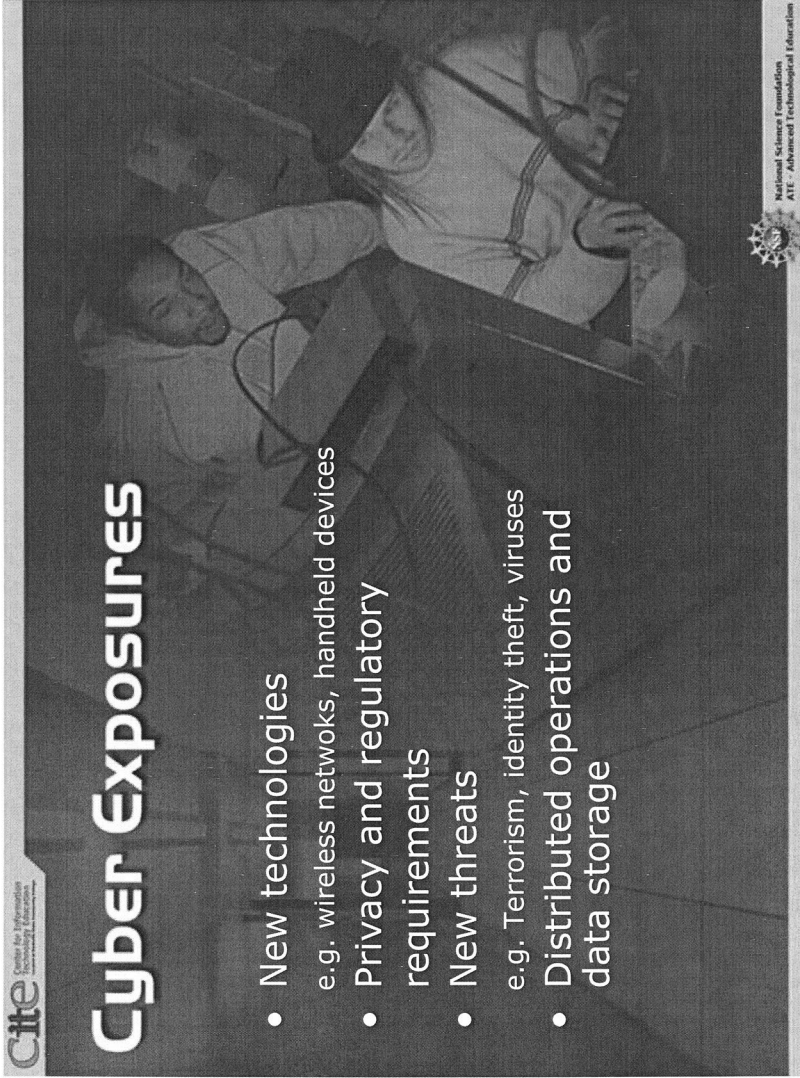
Cyber Exposures

- New technologies
  e.g. wireless netwoks, handheld devices
- Privacy and regulatory requirements
- New threats
  e.g. Terrorism, identity theft, viruses
- Distributed operations and data storage

National Science Foundation
ATE - Advanced Technological Education

Treatment of Cyber Exposures

- **Mitigation**
  - Patches
  - Virus protection

- **Reduction**
  - Firewalls
  - Encryption

Businesses today operate largely at the symptom level

National Science Foundation
ATE – Advanced Technological Education
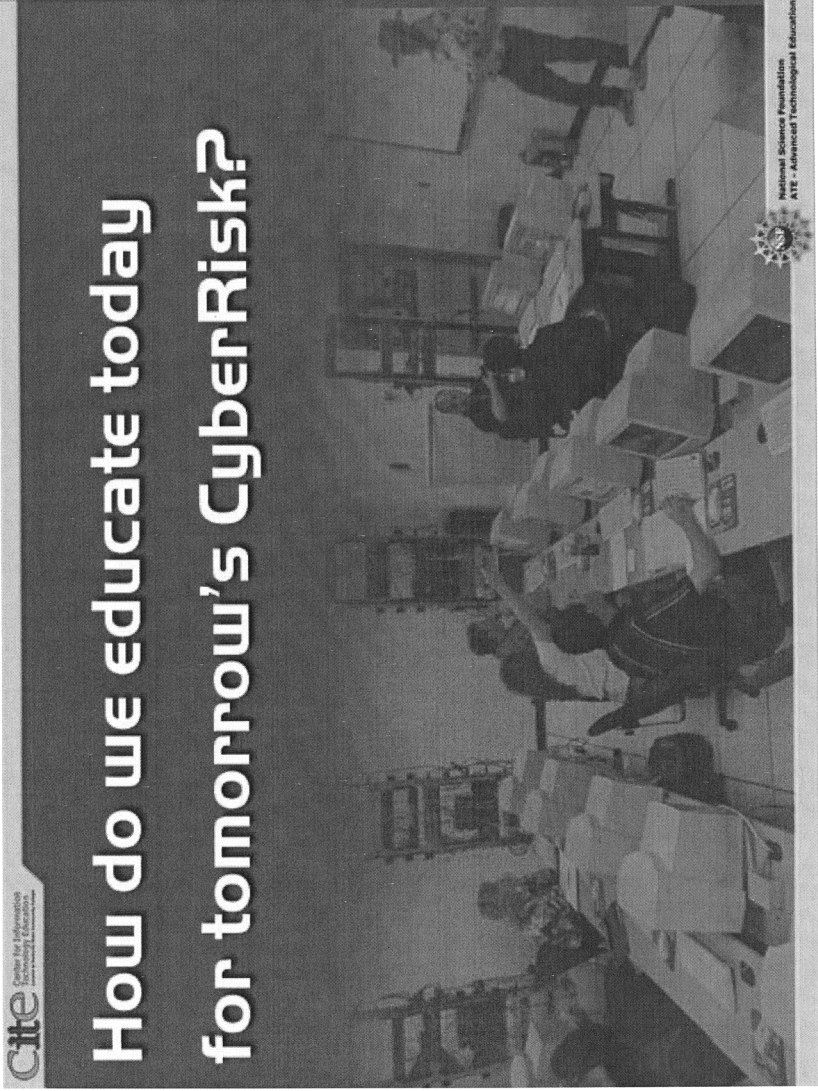
Education's response

- Certifications
- Adding course content
- New courses
- New concentrations
- New two- and four-year college degree programs

Network Consultant
Network Operations Analyst
Network Security Analyst
Network Security Consultant
Network Security Manager
Network Security Specialist

CompTIA Security+ – WFTC 0014

Security Overview and Authentication
Attacks and Malicious Code
Remote Access, E-mail and Web Security
Directory and File Transfer Services
Wireless and Instant Messaging
Devices, Media and Medium

National Science Foundation
ATE – Advanced Technological Education

Beyond curriculum, fundamental changes are required in our approaches to teaching and learning to improve critical thinking and problem solving skills

Learning in context

- Authentic experiences
- Business and industry participation
- Dynamic (not static) curriculum
- Strong linkages between content and application
- Teacher as facilitator
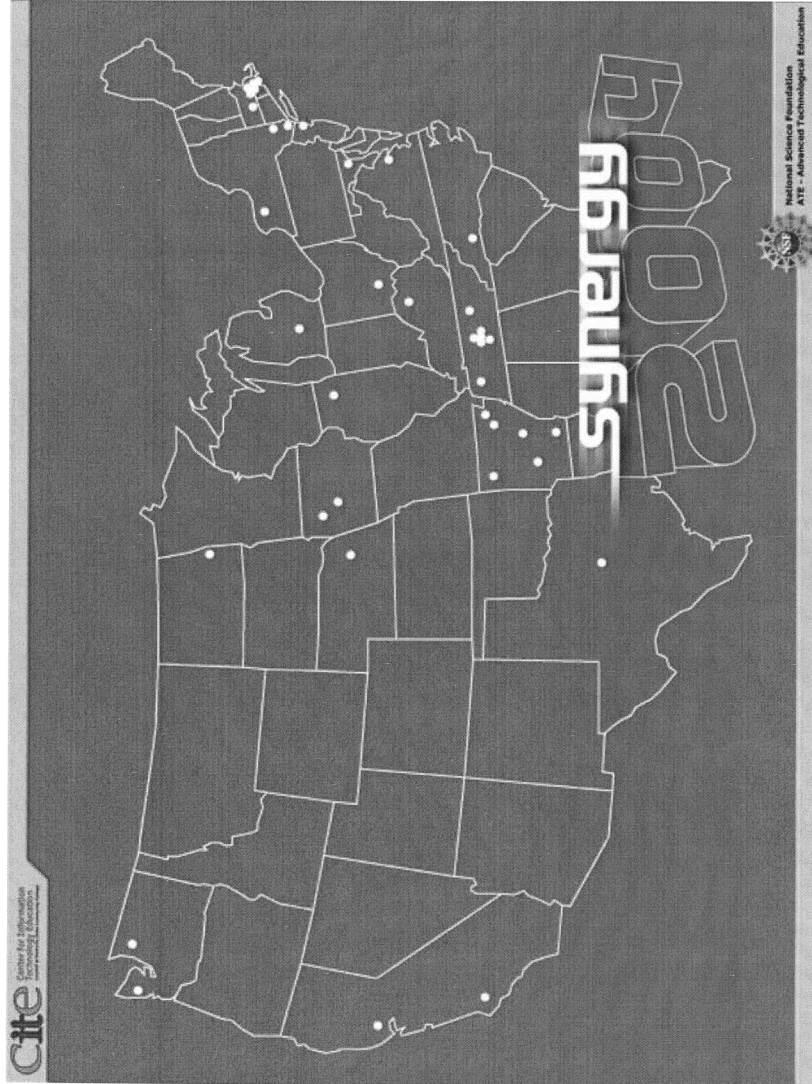
What can the government do?

- Provide incentives for business and industry to partner with community colleges
- Fund programs for student and faculty internships to provide real-world workplace experience
- Fund incentives to break down barriers that create educational silos
- Continue to support the NSF-ATE program to ensure currency of technical expertise and faculty development in community colleges
- Make technical education a national priority

National Science Foundation
ATE - Advanced Technological Education

BIOGRAPHY FOR SYDNEY ROGERS

Ms. Sydney Rogers is Vice President for Community and Economic Development at Nashville State Technical Community College where she is responsible for workforce development, distance education, student services, computer services, and grants and development. Prior to this role, she served as Interim Vice President of Academic Affairs and Dean of Technologies at Nashville State Tech where she was also Department Chair and Associate Professor of Computer Information Systems for 20 years. As Dean of Technologies, she was responsible for the overall success of 21 degree programs in Engineering Technology, Computer Technologies, Business, and Visual Communications.

Ms. Rogers serves as lead principal investigator for the Center for Information Technology Education (CITE), a regional center funded by the National Science Foundation, Advanced Technological Education program and has led four other NSF ATE projects. Her work has focused on the reform of technological education to create a more adaptable workforce suited for the new century. She serves on three NSF National Visiting Committees and several local boards. She has 30 years of leadership experience in technological education and workforce development.

NASHVILLE
State Tech

The Nashville Community's Two-Year College

July 16, 2004

The Honorable Sherwood Boehlert
Chairman, Science Committee
2320 Rayburn Office Building
Washington, DC 20515

Dear Congressman Boehlert:

Thank you for the invitation to testify before the Science Committee of the U.S. House of
Representatives on July 21, 2004 for the hearing entitled "**Cybersecurity Education –
Meeting the Needs of Technology Workers and Employers**". In accordance with the
Rules Governing Testimony, this letter serves as formal notice of the federal funding I
currently receive in support of my research.

Center for Information Technology Education
- $619,525.00, DUE #0202249, National Science Foundation, Fiscal Year 2002
- $589,601.00, DUE #0202249, National Science Foundation, Fiscal Year 2003
- $589,677.00, DUE #0202249, National Science Foundation, Fiscal Year 2004

The Case Files
- $299,820.00, DUE #0202397, National Science Foundation, Fiscal Year 2003
- $635,954.00, DUE #0202397, National Science Foundation, Fiscal Year 2004

Sincerely,

Sydney Rogers
Vice President, Community and Economic Development

DISCUSSION

Chairman BOEHLERT. Thank you very much.

When academics and business people and military people and
elected officials talk about a subject like cyber security, unfortu-
nately, too often, it elicits muffled yawns, because people aren't
really, sort of, focusing on it at all. Let me ask you this. Do we get
it and do they get it? Now the "we" is America, in general. Under-
stand the severity and the extent of the challenges facing us. And
do "they" get it? And I am talking about young people, like you, ob-
viously you get it, Lieutenant, and guidance counselors, on the
great opportunities that are available in this field. Let us talk
about in general, do they get it? Most businesses think their com-

puters are secure. Most individuals, and we have got them by the millions across America, have got all sensitive information about their personal finances and everything else on their home computer, and they think it is secure. Is it?

Mr. Hosmer, let me——

Mr. HOSMER. Actually, I don't think any of us get it. I don't think any of us understand the threat of a cyber attack, the stealing of our personal information at any level. I think that we are still struggling with this, because the threat is emerging. It changes every day at Internet speed, and we have to react to it. One of the ways we try to counter that to get it down into the high schools is we have created a high school internship program, not only at the college level, to basically bring high school students in to teach them what this is really about today. And those students are going on further in their education at the undergraduate and graduate level after leaving high school to understand this. So we have to train our young people to do that and understand what they can do about it. And it is an exciting career opportunity. When you look at television today and you look at programs like CSI Miami, etc., they are starting to excite young people about this particular career, because it has all of the sex appeal that they are interested in, and we need their help. And I think those programs are actually introducing new ways for people to get involved in these kinds of programs.

Chairman BOEHLERT. Lieutenant, you are nodding your head. When an officer nods to a non-enlisted guy, he says, "yes, sir."

Second Lieutenant APARICIO. No, I nod my head to the Congressman. But I just wanted to just add on to what Mr. Hosmer said that we do need programs, more programs in the sense that—to bring awareness. And I think one example is what we are doing right now in Rome, New York with the ACE program, targeting JROTC to bring the awareness to everybody. They tell their friends. They bring awareness, and that is just one less person that we have to worry about.

Chairman BOEHLERT. You know, everybody talks these days about identity theft. That is a big issue in America today. One of the easiest ways to be a very active and successful criminal in America today is to get a home computer and then go out and pilfer information from individuals on personal computers, from businesses, and—well, Mr. Baker, do you want to address that?

Mr. BAKER. I was thinking about your original question, too, about do we get it. And I think, on one level, we certainly do. I mean, if you don't—if you watch TV in any way, shape, or form, you, to some degree, get it. You know, there can be identity theft. There are problems. Businesses get it to some degree. Unfortunately, they sometimes get it a little too late. They get attacked by the most recent virus. They don't keep their software up-to-date to protect their systems and that kind of stuff. I think the more important issue is that the variety and levels of education that are needed and awareness—I mean, it starts with awareness building. And from there, it goes down to many deeper levels on the business side, the legal side, the computer science side where we can actually start building a cadre of professionals who can help protect us in many different ways, from the psychological, you know, who are

these people and why do they attack us, to the more physical, how do we protect our software, how do we protect the networks, how do we protect our computers—personal computers and that kind of stuff.

Chairman BOEHLERT. Mr. Spengler.

Mr. SPENGLER. I think when we look at the question of do we get it and do businesses get it, I am looking at what has been going on this year. And I think before this year started, I don't think a lot of businesses did get it. But with the proliferation of an enormous amount of viruses, business and industry now are spending more time on fighting those issues than actually enhancing and upgrading their networking systems. Unfortunately, the people that do get it are the people who are affected one at a time. It isn't almost until you are affected that you do understand the critical importance of the nature of it. What needs to be done is to focus on, again, and I totally agree with the processes of security awareness, but additionally, to focus on the policies and practices of companies being able to look at and address these types of issues.

From a curriculum standpoint at the community college, we are positioned very well to address from a practical skills and tools standpoint, these types of issues. Within our center, we look at the flow of curriculum as being a critical direction, being able to generate the new generation of practitioners from a general security understanding standpoint to more specific bridges in technologies to be productive in business and industry, such as the health care and financial industries.

Chairman BOEHLERT. Ms. Rogers, do you have any——

Ms. ROGERS. The employers that I have spoken with recently about this, in particular I have spoken with a senior executive in IT from one of the largest health care companies in Nashville, and I think that they get it. I think he gets it. I don't think he feels very secure. They are doing everything they can, but I think he thinks it is fragile, but—and I am paraphrasing—he said that we have got a dangerous combination, because the people who are working on cyber security understand it very well, those who are the professionals. But the—all of the other workers don't get it, and he—and his words were, "This is a dangerous combination."

Chairman BOEHLERT. Well, let me assure all of you that we get it on this Science Committee, but you would expect that this committee does, on a bipartisan basis. My bill, the Cyber Security Research and Development Act, was passed out of here, passed by the House and Senate, signed into law by the President. And that is very important, but you know, this room should be packed with representatives of the media. We have the specialty, technical press represented, but the popular media, so more and more people begin to appreciate the severity and extent of the problem.

When I was a young kid, I can remember vividly the Buck Rogers' stories. You know, a man on the Moon and everybody used to chuckle it would never happen. Last night, I attended the 35th anniversary of Apollo 11 when Aldrin and Armstrong walked on the Moon. And right now, it is not farfetched to think in terms if there ever is, God forbid, a World War III, it could be fought not with guns and bullets or ships or tanks or planes, but with computers. Our whole financial system, our transportation network, our elec-

tric grids, so much is dependent on a computer, so the subject here today is extremely important. And that is why we value so highly your testimony, and that is why we are focusing on education for the next generation, the Lieutenant Aparicios and those who will follow who will be on the front lines in this battle.

Thank you very much.

Mr. Gordon.

Mr. GORDON. Thank you.

Ms. Rogers, you have had experience with the NSF's ATE program and said it had been helpful at Nashville Tech. Can you give us any thoughts as to how that program can be improved in either content or administration?

Ms. ROGERS. I don't have any suggestions on how it could be improved in the administration, although, you know, I might if I thought about it longer, but to tell you the truth, I have been involved for 30 years in higher education in a number of federal programs and had a number of federal grants from different programs. And I have to tell you that as far as what is happening with ATE and technological education, it is of the highest quality. It is the best one that I have ever worked with. What I see as the problem, from my perspective, is that there are so many more community colleges who need help in this area, and you know, the funding pie is just what it is. So you hate to say just put more money there, but the fact is that there are a lot of good projects that are out there. Other schools want to participate with us and they just can't, because there is just not enough funding there. It is one of the—it is the best program, federal program, I have been associated with, frankly.

Mr. GORDON. Anyone else have any suggestions on improving the ATE program?

Mr. SPENGLER. From an NSF standpoint, administration, I think that NSF has—and the ATE, have been making solid steps with—to look at the collaboration between the different funded projects from NSF, which is allowing us to more broadly take in the work that has been done in specific projects and disseminate that work out to other schools that can benefit from the work. It is firmly our belief that without the NSF/ATE program, many of the faculty, quite frankly, couldn't afford the types of training needed to have quality programs within the schools, and many of the programs, absolutely, would not exist within these schools.

Mr. GORDON. We frequently talk about and hear good and bad about federal programs, but the NSF, I think more than anything else, is consistently given high marks in all regards. We are able to double the funds for NIH. I hope we are, at some point, going to be able to double funds over a period of time for the NSF. I think that is very, very important.

And Mr. Hosmer, in your written statement, you had talked about there should be a role, a federal role, in establishing national accreditation for cyber security education and training programs. You know, typically that is done by non-governmental entities. Could you elaborate more on why you think there should be a federal role here?

Mr. HOSMER. Actually, it is an excellent point. One of the things that we see is many of the training programs that are out there

that law enforcement, defense, corporate security take in order to basically make themselves current, they participate in these every year, and they spend a lot of money and a lot of time. And many of those programs come with continuing education credits from specific universities that are associated with that particular vendor's training program. Unfortunately, they end up with all of these ad hoc credits from, maybe, 10 or 15 different universities, and there is no way to bring them together in order to get a degree or any kind of overwhelming accreditation.

The second problem is that there are so many courses that are out there trying to understand the quality issues that are associated with each one of those programs and which ones to select and which ones to take because the investments are significant. What we are seeing in the marketplace today is typically $750 to $1,000 per day of, you know, advanced training in any kind of digital investigation or cyber security, plus the time and the travel in order to be able to do it. So you could easily spend $25,000 to $30,000 per year per employee in order to take these, and they come out of it with a certificate and not with any kind of degree from——

Mr. GORDON. Those are legitimate concerns. I guess my question, though, is why—or what would be a federal role here where typically it is, you know, a non-governmental accreditation body that does those sorts of things?

Mr. SPENGLER. I think the government role can be one of coordination, one of bringing together those universities that are accrediting all of these courses out there and trying to come up with some sort of national program, not to basically administer it, but actually to coordinate it, to hold more hearings on how to bring those things together so that the universities and industry partnerships can be formed so that we can solve this basic problem. It is not being solved by the universities by themselves or the industry partners by themselves, and it needs some sort of organization that can basically help bring that together.

Mr. GORDON. Anyone else have any—yes, sir.

Mr. BAKER. I look at it as two different issues. One is accreditation. And I understand where you are coming from. If you look at the model where business programs are accredited, that is somewhat of a private institution, ACSB, those accreditations, so to speak, for business programs, and I think that is the kind of context in which your question is coming out. You know, shouldn't we have that kind of model for accreditation for security programs? But I think the first step to that process is creating standards in education, looking at the variety of education needs from the end user in a particular discipline, be it medicine or manufacturing or whatever the area is, and the levels of people. Some staff just need to be aware of what is going on, and to know that they should be thinking about security, all of the way to the more technical level where we look at software development and the issues of applications development to security and network development and the security that goes with those kinds of things. You know, in the classroom, we often joke with the students about, you know, how are you securing your log-on to a particular system, you know. You put in a very difficult password and user ID, but in point of fact, you can't remember it, so we go to putting it on a little piece of, what,

paper and sticking it next to your monitor and, you know, gee, no one would think to look there to find the user ID and password. You know, those kinds of things. Be aware of not doing those things. You know, from awareness all of the way down to the more technical levels. So I think it starts with, you know, what kinds of security education needs to be done, what kind of standards should apply to that at what levels in different disciplines, and then look at accrediting different kinds of programs, because they—there are different needs at different levels.

Chairman BOEHLERT. Thank you very much. The gentleman's time has expired.

The Chair recognizes the distinguished Chairman of the Subcommittee on Research, the gentleman from Michigan, Mr. Smith for five minutes.

Mr. SMITH. Mr. Chairman, thank you.

Really an exciting hearing in terms of the potential for problems that we have already looked at. It seems to me, though, that a country, such as the United States that probably has a greater dependency on the Internet and computer systems and the fact that the inter-connectedness of these systems, whether it is banking or food distribution or the military or airlines or anything else, big corporations, the military, the inter-connectedness is very important because of the usefulness. And it seems to me that that brings in two questions, not only the cyber security and the potential for damage because of the inter-linking of the computers, but also the physical, potential physical damage that could be done to central servers. So part of my question, Mr. Baker and Mr. Hosmer and maybe Lieutenant, is should there be or is there any consideration for somewhat of a confidential setting for the server systems that might be more vulnerable to physical attack?

Mr. BAKER. The short answer is probably yes. The longer answer is look at some of the protection systems that have been put in place by various organizations. If you take the events of September 11 and look at what occurred on September 11, the computer systems in point of fact were ready to go fairly quickly after that occurred, because they had already—most of the financial industry, which is highly dependent on network information systems, had their systems off-site, remote locations, not easy to get to in one single attack. They recognize disaster recovery planning and the needs for it. So they were somewhat prepared.

Mr. SMITH. So are you saying that most of these systems, whether you are a large corporation or a financial institution, the way we move money or move materials or move airplanes or move personnel, that they have more—they have several servers that can accommodate the damage to any one single facility server? I sort of was under the impression that a lot of these corporations and the people that—where they outsource server networking accommodations are centrally located.

Mr. BAKER. Some organizations will. Most of the medium to larger sized organizations will have backup systems. They will do remote off-site storage. There are a number of organizations that provide off-site storage capability in various parts of the country and recovery capabilities in various parts of the country. And some organizations have redundant systems where——

Mr. SMITH. How serious would be the physical damage of a car bomb, an Oklahoma type bomb or a bunker buster type bomb, to a large, central server center that does work for even—either—for anything?

Mr. BAKER. My guess would be probably down for a day or two, but if it is any sizable organization, they recognize the need for, again, disaster recovery planning and have probably put in place the ability to get back up fairly quickly. You know, one of my former roles, before I came into education full-time, was to run an IT organization for a large group. And the issue that we addressed most importantly was disaster recovery. And we had put in place the ability to get back up and running within a day or two.

Mr. SMITH. Mr. Hosmer, at Utica, or Mr. Baker, at Johns Hopkins, what would be the salary for an individual graduating with a Master's degree in—specializing in cyber security?

Mr. HOSMER. Well, that certainly depends, you know, on the job that they are going to take, but the starting salaries out of those are certainly in the $50,000 to $75,000 range in our region for graduates, and that could be higher in other parts of the country, certainly, but as a starting salary, that would be very typical.

Mr. SMITH. So if a terrorist organization that didn't look like a terrorist organization offered $150,000, they probably could hire the greatest talent that might be graduating?

Mr. HOSMER. Just about anybody they wanted to, sure.

Mr. BAKER. Okay. Now your point—the previous question that you asked is that, you know, we tend to think about cyber attacks or attacks on the physical infrastructure from the outside in. The greater threat is from the inside out. The insider threat that we have to counter inside our organizations and the trust that we put in people that have access to those systems. And in, typically, most organizations, it isn't one person that has the keys to the kingdom; it is typically multiple people in the organization that have keys to the kingdom. Everybody has root access in order to be able to access those systems and modify them. So the real threat, from a cyber security perspective, is the insider threat, and we focus most of our attention on the outsider threat where, in fact, we need to turn more attention to the inside.

Mr. SMITH. Will your graduates—concluding, Mr. Chairman. Will your graduates or—Lieutenant——

Second Lieutenant APARICIO. Aparicio.

Mr. SMITH [continuing]. Aparicio, will their talents and what they learned be obsolete because of the technological advances that are taking place in computers? And it is such a changing evolution, it seems like, just in the last 10 years of what has happened in research and science and computers, will what we are learning now—is it continually being updated for a person that wants to be in that field? Lieutenant——

Second Lieutenant APARICIO. Sir——

Mr. SMITH [continuing]. Are you going back to refreshers every six months?

Second Lieutenant APARICIO. Oh, well, I was going to comment on that. We have to—as military members, we are always being trained, having required reading courses, and it is just part of professional education to keep up. And as—to answer your question

about the graduates, I don't believe that they would be obsolete if they keep on learning. The students that we target, they are not necessarily what I would say the average, but there are requirements, and most of them have higher aspirations to continue on learning. I think that that is true for most people who—you know, you don't just stop learning right after high school. You don't stop learning after college. To keep up——

Mr. SMITH. Sometimes when you get to Congress, it slows down a little bit.

Second Lieutenant APARICIO. I wasn't implying that, either, sir.

Mr. SMITH. Thank you, Mr. Chairman.

Chairman BOEHLERT. And that is why we invite expert witnesses like that to continue to be teaching.

The gentleman from Washington, Mr. Baird.

Mr. BAIRD. Thank you very much. I thank the Chairman for hosting this important meeting, and I thank the panelists.

I had the coincidental good fortune of riding on the flight here with the gentleman who wrote the security standard for wireless Internet technology. It is one of those great serendipitous things. And I asked him to look at some of the issues today. And I thought his comments were interesting. He personally suggested to me that the notion of a certification exam probably was going to be obsolete before you actually—by the time you have created the exam, the world of real-world change has probably exceeded the exam, so he didn't think we should spend a lot of time on that. And certainly my experience, which is limited, but—would suggest that may be the case.

Two questions I have, one from him and then one of my own. He expressed a challenge that academics often have a difficult time working within the government setting, and within, more importantly, perhaps, with industry. So you have got the academics, the cryptographers, etc., working on the mathematical equations within the academic institutions, but then you have got the people working on the standards within industry. And one of this gentleman's claim to fame was he basically broke into the initial wireless standard in about 30 seconds flat. He just looked at it and said, "You have got a huge flaw here," because basically the folks doing the industry side were the guys working on the radio side of it and the broadcast side of the—of wireless, and he was looking at the cryptographic issues. So the question I would have is what obstacles do we face in terms of interactions between the academic side, the government standard setting side, and real-world industry that is creating the hardware and software that we use, and how can we address those?

Mr. SPENGLER. I would like to address just—the obstacle we face is the complexities of developing quality faculty and spending those times becomes difficult when you are looking at practical experience. Sometimes we look at developing those skills and then we bring those skills to the classroom. But for faculty to really be effective and efficient within the classroom environment, they need to understand the applications of technologies out in the workforce. It is our belief that the encouragement of faculty participating in real-world work experiences is critical to the ongoing development, not just the attending of courses, to build a finite set of skills that

might be changed in a quick manner. What we try to encourage is to establish relationships with business and industry not just to look at the concept of students being able to go out in the professional development environments but for faculty to participate. For example, we are working with a hospital called Gotlieb Hospital in the Chicago area and implemented voice-over wireless within the hospital. So we approached them, and we are working on a partnership with this hospital, and again, we are trying to model that throughout the Midwest for us to be able to identify meaningful projects that are going on out in industry and to be able to schedule those and including faculty as part of those projects. What we are finding that is very interesting is that in many times—in many cases, faculty are actually able to excel in those areas because of their detailed knowledge of the actual technologies and they are actually able to offer a lot to business and industry at the times they are participating in this type of externship opportunities.

Mr. BAIRD. Great example.

Ms. Rogers.

Ms. ROGERS. I would like to address that, too. The basis for almost all of our work at our NSF project has been to develop what we call contextual problems, but it is all based on authentic workplace experiences. We have two kinds. One we call problem-based case studies where current problems in industry are brought into the classroom. But even in more recent types of authentic experience we have the students actually solving industry problems, real-time in working with the industry. And we think that we have to make that a part of the curriculum development process so that we have a dynamic curriculum development process.

Mr. BAIRD. That makes sense to me.

Ms. ROGERS. And the other thing that I think is relevant here is that the whole issue of retraining that comes up in understanding new information, what we have worked on, and education research supports this, is that we know how, by structuring the learning environment the right way, to create workers and employees that are more adaptable. We know—we have evidence of how to make people transfer knowledge better from one situation to new situations based on the way that they are taught. So if we can further that effort and teach them differently, we can create a workforce that is more adaptable, and therefore more able to understand the new stuff as it comes out.

Mr. BAIRD. Thank you.

Mr. Baker.

Mr. BAKER. Yeah. One of the things—a couple of things that come to mind, you know, one, the question of, you know, can we keep up with the technology as it is evolving, and to some degree, yes. And that is a little bit of the difference between training and education. We look at education as the process of teaching a student how to learn so that they can keep up on their own. You know, training is learning how to do something very specific. Education is teaching how to learn, how to do information literacy, how to research things, etc. And a second comment, along with the ones that Ms. Rogers was making, that you know, in our programs, we have the same kind of—I don't want to call it experiential, but completion part of our program where at the end of their degree, we

like to characterize it as you need to see where the rubber meets the road. Okay. Here is what you have learned in the classroom, now let us take it out into the practical world. So we have a senior project where students over, roughly, a 20-week period of time are doing projects for organizations or doing some applied research for organizations, etc., so that they can take what they have learned and then see how it really works, you know, from the real-world perspective, so that they can understand the translation of yes, I learned this theory and sometimes it doesn't work, but sometimes it does, and here is how I can improve things.

Mr. BAIRD. Mr. Chairman, I know my time is expired. I might, if I may—I appreciate those answers. The one thing I would say— the question I was going to ask, but I know I am out of time, but for a future reference——

Chairman BOEHLERT. You can ask the question. Go ahead.

Mr. BAIRD. Well, it is—oh, he is gone. Okay. The question is this. My understanding is that increasingly chip fabrication facilities are locating—they have been, for a long time, locating offshore in Taiwan, but now increasingly on Mainland China. The fabs are going there. Increasingly, we know that we are outsourcing code writing, and I have a two-part concern as this relates to cyber security. One, are we losing or is it—maybe is it eroding our technological, educational, academic base of expertise in these areas so we are going to get more and more people with more expertise abroad than domestically? And two, is code written or hardware developed offshore posing a security threat that we need to be cognizant of?

Mr. HOSMER. That was what I thought your question was originally, and I was going to address that. I mean, obviously most of the vulnerabilities within systems today are vulnerabilities caused by bad software. Okay. And the reason is that security is typically an afterthought, not a forethought, in the process of developing these systems. Further complicating it are your exact points of moving most of the software development offshore. The estimates are the next version of Microsoft Windows is going to have 100 million lines of code. If you think about 75 or 80 percent of that being developed offshore, and this is the critical infrastructure that we are basing our Nation on, it is certainly a risk to be concerned about, because it is impractical to walk through every line of software in those systems in order to be able to address the threat. So we have to come up with a better way, and that goes into training and education to build better software, but also how do we assess and analyze that in order to basically determine if it is safe.

Mr. BAKER. Yeah, one of the things I would say is it also is a matter of jobs and students going into programs wonder if there is going to be a job coming out, and to some degree, the answer is no, and so they think of other things to do.

Mr. SPENGLER. I would like to add one more item on that. We initially started our center focusing on predator protection and information assurance. And one of those—one of the issues that quickly came up was the idea of secure coding. When taking a look at the available programs in secure coding, we found that there wasn't a lot currently out there as far as structure and secure coding environments. We contacted some professionals in the industry, and they concurred, and that is one of the directions of secure cod-

ing. Does it pose a risk if those jobs and that software are moved offshore? My answer would be yes.

Ms. ROGERS. One of the employers in Nashville said that secure coding is worse than Y2K with no end in sight.

Mr. BAIRD. Expand on that, if you would, Ms. Rogers.

Ms. ROGERS. Well, he sees the problem as, you know, especially in the legacy systems where what we are trying to do is protect and just sort of patch what has already been developed out there, because those systems weren't developed with security in mind. And so if we think about developing the future workforce so that they can develop our new systems and doing so with security in mind is part of the design on the front end, but then if you add the issue of taking those jobs offshore, then you have really got a problem, as you pointed out. I mean, he—and he said that this problem that we are dealing with the legacy systems all over the country is—it—I think that—his word wasn't fragile, but that was what he meant.

Mr. BAIRD. I appreciate that we now know a new problem. I don't know that we will get the solution in today's hearing, but it is——

Chairman BOEHLERT. Thank you very much.

Well, I will wrap it up with sort of a two-part question. The first part is do we know the extent of the challenge? And it has been suggested by many that entities, whether they be private sector businesses or public sector government, are reluctant to share information about their vulnerabilities. And so we really probably don't know the extent of the problem. And secondly, what do we do? How would you suggest we do something to promote a national awareness program so that the individual, the business, people across the broad spectrum will appreciate that this is a very serious issue facing the Nation at a critical time and we better darn well be responsive in addressing the issue? Two-part question. Do we know the extent of the problem and how do we increase public awareness so that—well, that is enough.

Mr. Hosmer or anybody?

Mr. HOSMER. Well, I think the extent of the problem has always been an issue. It has always been underreported, because of the concern that it would have on the organization. Legislation, like Sarbanes-Oxley, that has been passed that requires the reporting of those kinds of things and that will go into effect on November 15 of this year, are going to require at least publicly-traded corporations to provide public data about those threats, also about audits and other things that could have been modified. So that is a step in the right direction, so there is going to be more full reporting, at least from publicly-traded companies, on those kinds of impacts. But there is still a lot that is not going to be reported. And I think without that reporting and understanding of the problem and the sharing of that information, everything in this area has been underfunded because of that. I think the awareness issue is attempting to be addressed through conferences and workshops that are popping up everywhere in the country. I have seen an increase in participation and the number of those over the last two to three years. They have been significantly increasing from virtually every aspect of our community. And the attendance, because we go to all of those, has been significantly up. So that is hap-

pening automatically through the normal channels, but it is certainly still not enough. I mean, we still need to get this information out to people to talk about the threats about the vulnerabilities that are out there and encourage some sort of national communication and reporting of the problems that we face.

Chairman BOEHLERT. You know, I recall a conversation I had a few years ago with an executive of a credit card company, who, at that time, and this was maybe eight years ago, told me that his company's experience—well, they lost, on average, about $100 million a year due to fraud, most of which was perpetrated using cyber systems. And he said his company concluded that was an acceptable loss, because it would probably cost them more than that to prevent that loss. And I said to myself, just like me, Americans have a lot of plastic in their pocket. And we are paying interest rates higher than we should pay, because we have to cover that fraud and that loss. So it affects every single person in a variety of ways.

Mr. Baker.

Mr. BAKER. It is interesting you would mention that, because you know, one of the thoughts that came to my mind when you talked about awareness programs, to some degree, business is doing it for us. You look at the Citi Bank ads with identity theft. You know, they are hard to forget, because they are so cute, but they drive the point home, "Be careful about the information about you," which is an awareness program. It is an awareness campaign. Taking it to other levels and other areas is another story, you know, protect your computer and that kind of stuff, you know, because it is only about protecting the credit card that you have. To some degree, legislation that has been passed has already helped. I mean, HCFA [Health Care Financing Administration] is raising awareness in the medical area. Sarbanes-Oxley, as Mr. Hosmer has already indicated, is going to certainly raise awareness in the private sector of what we have got to do. To some degree, I don't think they quite understood yet what it really means, but it certainly will hit them square in the face, you know, when they start getting questions about their finances. And business, to some degree, and you have already kind of expressed this, looks at it as a cost of doing business. So if it costs me $300 million to put in security and I lose $100 million, on balance, I will pay the $100 million instead of $300 million.

Chairman BOEHLERT. But you don't pay the $100 million, we do.

Mr. BAKER. Right. That is correct.

Chairman BOEHLERT. Anyone else care to—Lieutenant?

Second Lieutenant APARICIO. Sir, I was going to try and answer a comment on both of those questions, and the—to the point on the knowing the extent of the challenge, I think we know the challenge, but America does not necessarily understand the challenge. But the people who really do are the younger generation. And so for, like a lot of people, they say, "Well, I can't fix my computer, but my son does," or "My daughter can fix it, because I don't even know what is going on." And so again, that shows that we understand that the younger generation has more of a command on that. And what we need to do is be targeting that next generation who is going to be running everything around here soon and educating

them. And how we, again, could help out is just, as mentioned earlier about the Citi Bank or credit card commercials that we see that we laugh at, we need to be, probably, doing some sort of announcements or putting it on TV where we all can watch and see the extent of it. You know, just like a simple, "Would you park your car in DC unlocked? Well, then why do you have your network," you know, "running open, too?" You know.

Chairman BOEHLERT. Sure.

Second Lieutenant APARICIO. Just things like that, but I would just say we need to be targeting the younger generation.

Chairman BOEHLERT. Well, let me say we agree with that wholeheartedly, and we are comforted on this committee and in Congress when we see young people like you with your very impressive record and direction in which you are going. And you are reflective of so many more that are with you and doing what you are doing. We just need more of you.

Second Lieutenant APARICIO. Thank you, sir.

Chairman BOEHLERT. Anyone else? Mr. Baker.

Mr. BAKER. I—yeah. Interesting you were talking about the younger people, and I agree with that about the grade schools and the high schools, and it is kind of anecdotal information, but it kind of drives home the point of how much the younger generation understands technology. My son is here today, and one of the things I talked about in my class about him, he doesn't know this yet, is that in the fifth grade, he did five PowerPoint presentations that year.

Chairman BOEHLERT. In the fifth grade?

Mr. BAKER. In the fifth grade. And the next year, he wanted to stop doing those and go back to doing poster boards, because it was a lot of work. But I think it underscores just how much technology that the younger generation understands. He likes to get on the Web. What does he like to look for? Game codes so that he can figure out how to get through his video games faster and get more advanced——

Chairman BOEHLERT. Mr. Baker, that allows me to get an applaud for something this committee has done. We are responsible for the science and math initiative for America, because we look at the international comparisons. And our youngsters, when compared to their counterparts around the world in math and science proficiency, if you issue a report card, there is need for improvement. The fourth graders are about on par with their counterparts around the world in math and science proficiency. The international comparisons show that by the eighth grade, we are falling a little bit behind, and by the twelfth grade, we are way down on the list. That is not good enough for America. So we, in this committee, the Science Committee, Democrats and Republicans working together, added to the No Child Left Behind big education initiative, something that is called the Math and Science Partnership Program. We are determined to do a better job of producing more people like Lieutenant Aparicio, because if we fail on that mission, shame on us. We are not going to fail. We are going to succeed.

Does anyone else have anything for the good of—Mr. Hosmer.

Mr. HOSMER. Just one final point on your—the acceptable losses from the credit card companies. The reason that there can be no

acceptable losses, regardless of who is paying the bill, is because where are those funds going that have been stolen, because criminal organizations and terrorist organizations attack those infrastructures in order to fund their other operations? And I think that we have to look at all of those losses and find out where they are going, because they may be going into a place that none of us would accept, regardless of how small the losses were.

Chairman BOEHLERT. Thank you very much.

I wish the media would beat a path to the door of the boot camp, cyber security boot camp up in Rome, New York. This year, they have got about 28 Aparicios up there, and they are the best and the brightest from all over the country. They have such a promising career path ahead of them, and as you have observed in the upstate region, you know, a graduate starts at $50,000 to $75,000. That is not a bad start. And the future is virtually unlimited for them, so we have got to do a better job of advising more people of the great opportunities and also heightening the awareness of the American public on the challenges that face us.

And you have been facilitators for this committee in that regard, and I thank you all for your testimony. This hearing is adjourned.

[Whereupon, at 11:35 a.m., the Committee was adjourned.]

Appendix:

ANSWERS TO POST-HEARING QUESTIONS

Responses by Chester "Chet" Hosmer, President & CEO, WetStone Technologies, Inc.

Questions submitted by Representative Bart Gordon

Q1. In general, what is the state of credentialing for cyber security professionals?

Q1a. Are there certification standards in place or under development for cyber security education and training programs?

A1a. Certification today comes in basically two flavors: Formal training courses held for law enforcement, such as those held at the Federal Law Enforcement Training Center (FLETC), and the International Association of Computer Investigative Specialist (IACIS). These courses offer certifications that carry significant weight in the community. The second is courses being offered by commercial organizations offering certifications. These certifications are offered by the hosting organization. Typically the certification requires the participants to take a test that is a combination of a written test and a practical examination.

Q1b. Do formal mechanisms exist to develop such standards, and if so, please describe how they work?

A1b. Certainly on the federal level, certifications offered by FLETC and IACIS are reviewed by advisory boards. In the commercial sector, a similar model is put in place by organizations offering the training. However, the acceptance of these credentials is based primarily on the respect for the organizations offering the training, which is based on the perception in the marketplace.

Q1c. To what extent are academic credits for cyber security studies earned through programs at one institution transferable to another in furtherance of meeting degree requirements?

A1c. Several organizations (WetStone being one) have entered partnerships with colleges and universities to offer continuing education units (CEU's) for students completing training courses. Here in New York State, the formula is typically .1 CEU per contact hour. Therefore, a two-day—16-hour training course would yield 1.6 CEU's. In our case, our instructors, course materials, and curriculum are reviewed by the college and then approved. Periodically, professors will sit in on one of our courses and provide feedback and suggestions. The use of these CEU's is an important consideration, and my suggestion is to establish criteria for national recognition of the CEU's that would allow these credits to be applied more easily toward degree programs.

Q1d. Is there a federal role in establishing national accreditation of cyber security education and training programs, and if so, how would you characterize it?

A1d. I believe the advancement of cyber security education and training is an essential ingredient in improving our nation's cyber security posture. The Federal Government has an opportunity to work with, and bring together colleges, universities, training organizations and those charged with the protection of our critical cyber security resources, to help establish standards and accreditation for professionals at all levels. I would recommend the establishment of a working group that could, within a short-time (12 months), study the situation further and deliver a report to the House Science Committee with recommendations regarding the needs, impact and nature of such a national accreditation.

Q2. What is the supply and demand situation for individuals with cyber security expertise? What evidence do you have that such individuals are in demand, and what skill sets are most in demand?

A2. Today the investigation of cybercrime activities is at an all time high. Virtually every law enforcement organization in this country has increased their backlog of cases involving digital or cyber evidence. The law enforcement agencies that we work with are constantly seeking assistance, new technologies and methods to speed the investigative process, and additional human resources to interpret the results. Today more and more digital evidence relating to both traditional and cybercrime activities enters U.S. Courtrooms. The need for highly trained cyber security professionals that can collect, analyze, interpret and report on cyber activities is upon us. We must rapidly expand this cyber security workforce with individuals that are not only talented, skill and dedicated, but also bring a high degree of integrity and ethics to the process.

Answers to Post-Hearing Questions

Responses by John R. Baker, Sr., Director, Technology Programs, Division of Undergraduate Education, School of Professional Studies in Business and Education, Johns Hopkins University

Questions submitted by Representative Bart Gordon

Q1. In general, what is the state of credentialing for cyber security professionals?

Q1a. Are there certification standards in place or under development for cyber security education and training programs?

A1a. While there are some recognized credentials for information security professionals, there is no widely recognized, independent credentialing organization or process currently in place. Unlike accounting and other professions, the 'standard' is to recognize credentials offered by companies established to do the credentialing. ISC², CompTia and SANS are the most widely recognized organizations providing such credentials. Each has some 'standards' for their credential and a course intended to prepare the professional to take the credentialing test, which they also provide.

Q1b. Do formal mechanisms exist to develop such standards, and if so, please describe how they work?

A1b. I am not aware of any formal mechanisms currently in place to develop fully independent credentialing for security professionals at various levels.

Q1c. To what extent are academic credits for cyber security studies earned through programs at one institution transferable to another in furtherance of meeting degree requirements?

A1c. The typical arrangements are for one institution to accept credits from another accredited institution. Academic institutions in the U.S. are accredited by a regional accrediting organization, sanctioned by the Dept. of Education. (Johns Hopkins is accredited by the Middle States Accrediting body.) However, each institution usually reserves the right to not accept credits from another institution, usually, because 1) the number of credits to be transferred in for a student exceeds some limit, 2) they are not applicable to the program the student will be entering at the new institution, or 3) there is some question of validity of the sending organization or the credits.

Also, if the organization that is providing the credits is from outside the U.S., another process is in place to determine the validity and applicability of the incoming credits.

Q1d. Is there a federal role in establishing national accreditation of cyber security education and training programs, and if so, how would you characterize it?

A1d. At the moment, the federal role should be reserved to encourage the industry to develop an independent set of credentialing criteria. This could be accomplished through some small grants intended to start such a process, and/or the development of specific standards within the Federal Government for various levels of security professionals. Credentials should be tied to specific job task or employment requirements. NIST has done some work in this area.

Once the credential requirements are established and the process for determining if a professional has met the credential requirements is in place, the industry can usually provide plenty of opportunity to receive the appropriate training or education needed to receive the credential.

Q2. What is the supply and demand situation for individuals with cyber security expertise? What evidence do you have that such individuals are in demand, and what skill sets are most in demand?

A2. Anecdotal evidence suggests the will be plenty of opportunities for security professionals. Network security appears it will be the most sought after expertise in the near future.

Q3. You indicated in your testimony that NSF has not been able to support innovative initiatives in information security education because of funding issues. Could you expand on this comment, and in particular, what kinds of innovative initiatives are not getting support?

A3. In discussing this issue with colleagues, they have indicated their understanding is NSF has not received its full funding and therefore is not able to sup-

port some proposals in the area of cyber security education. However, they did not provide specific information about their concerns.

Q4. What has been your experience with the NSF Scholarships for Service program in terms of its ability to attract good students and its success in placing graduates in federal agencies? Do you have suggestions on ways to improve the scholarship program?

A4. Hopkins' experience with the SfS program has been good. Earlier we had some problems placing the students, but that seems to be much less of a problem at this point.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Erich J. Spengler, Principal Investigator, Advanced Technology Education Regional Center for the Advancement of Systems Security and Information Assurance, Moraine Valley Community College

Questions submitted by Representative Bart Gordon

Q1. In general, what is the state of credentialing for cyber security professionals?

Q1a. Are there certification standards in place or under development for cyber security education and training programs? Do formal mechanisms exist to develop such standards, and if so, please describe how they work?

A1a. The current state of credentialing encompasses an ongoing debate regarding the modeling of curriculum on industry certification. This debate focuses on the balance between certification standards and required skill sets. As academic institutions construct the basis for cyber security curriculum, several factors must be considered. These factors include the reflection of current industry demand identified by job skill proficiency and alignment to existing standards or certification through government or private entities. Therefore, one set of standards is not in place, but the debate for its development is indeed ongoing.

Job skills proficiency and the mastering of industry knowledge often represent the framework used to construct cyber security programs from a practitioner outcome perspective. Cyber security skills are often identified through a thorough examination of current and future employer hiring needs. This process is often costly and must be ongoing to ensure consistency with current employer demands. Failure to accurately represent needs may result in programs that lack necessary components to adequately prepare cyber security professionals. To avoid these situations, many vendor and non-vendor organizations have established education/training programs and certification processes for benchmarking information security knowledge.

I would caution the use of the term *certification standard* at this point, as this may convey that a single model of authority exists. In fact, there are currently many available models that can be used when creating cyber security education and training programs. The following represent only a few of the models that developers evaluate when establishing their curriculum framework:

(1) *The International Information Systems Security Certifications Consortium, Inc. (ISC)[2]*

(ISC)[2] maintains what is referred to as the Common Body of Knowledge for Information Security (CBK). They administer certification examinations and require the maintenance of post certification credentials through continuing education. The CBK provides a common foundation for the mastering of information security skills. The Certified Information Systems Security Professional (CISSP) and System Security Certified Practitioner (SSCP) are certification examinations offered to candidates wishing to demonstrate proficiency in areas of CBK knowledge.

(2) *The National Security Agency/Central Security Service*

The Committee on National Security Systems (CNSS), chaired by the Department of Defense, works with the National Information Assurance Education and Training Program (NIETP) to develop Information Assurance training standards. Under these standards, the Information Assurance Courseware Evaluation (IACE) program is used to ensure compliance with national standards including:

NSTISSI 4011	INFOSEC Professionals
CNSSI 4012	Designated Approving Authority
NSTISSI 4013	System Administrators in Information Systems Security
NSTISSI 4014	Information Systems Security Officers (ISSO)
NSTISSI 4015	System Certifiers

CNSS and (ISC)[2] are examples of the many groups that are working to provide standards in information security education and training. Others include the SANS Institute Global Information Assurance Certification (GIAC), CompTIA Security+,

the National Institute of Standards and Technology (NIST) Special Publication 800–16. Additionally, vendors such as Microsoft, Cisco Systems Inc., and IBM develop product-specific and technology-specific security certifications. A growing challenge exists when determining which of the aforementioned certification standards should be incorporated as curriculum is mapped to certification.

The National Security Agency (NSA) currently implements the Information Assurance Courseware Evaluation (IACE) Program. This program enables cyber security education and training programs at academic, government and commercial organizations and most recently community and two-year technical colleges, to map curriculum to national standards as set forth by the Committee on National Security Systems (CNSS).

The National Science Foundation Advanced Technological Education (NSF ATE) program continues to play a major role in the identification and development of appropriate standards for education and training programs in cyber security related areas. The NSF ATE program also encourages collaboration between organizations tasked with the formulation and development of such standards. Over the next year, the NSF ATE Regional Center for Systems Security and Information Assurance (CSSIA) will partner with the National Workforce Center for Emerging Technology (NWCET) to enhance and review current skill standards. This group will also determine opportunities for alignment with other skill standards identified by (ISC)², CNSS and others.

Q1b. To what extent are academic credits for cyber security studies earned through programs at one institution transferable to another in furtherance of meeting degree requirements?

A1b. There is a clear weakness in the transferability of academic credentials from one institution to another. With a lack of common standards for program certification, schools construct programs reflecting different standards. Some programs may place an emphasis on a particular vendor's cyber security skill requirements while others may emphasize a more general non-vendor approach. This results in curriculum that is difficult to articulate on a course by course basis resulting in earned credits not transferring. When earned credits do not transfer, barriers emerge for students as they continue the pursuit of cyber security related careers. Institutions should be encouraged to emphasize a common set of standards or certification criteria in cyber security. Through this, academic education and training programs will substantially increase pathways toward articulation.

As noted in my original testimony, community colleges play a critical role in the education and training of the Nation's workforce. The American Association of Community Colleges (AACC) also indicates that community and technical colleges enroll 44 percent of all U.S. undergraduate students, including 11.4 million credit and non-credit students. From these numbers, some 200,000 certificates and 450,000 associate's degrees are granted each year. As cyber security programs emerge we must consider that the ability to meet degree requirements will be significantly reduced without emphasizing pathways, articulation agreements, and common standards. The NSF ATE program supports projects that provide guidance and leadership in the area of career pathways, articulation and standards. NSF ATE Centers continue to focus on these initiatives.

Q1c. Is there a federal role in establishing national accreditation of cyber security education and training programs, and if so, how would you characterize it?

A1c. The Federal Government can play a role in the national accreditation of cyber security education programs. Most recently, inviting community and two-year technical colleges to submit requests under the National Security Agency (NSA) Information Assurance Courseware Evaluation (IACE) Program is a move in a positive direction. We must, however, recognize that the acceptance of other standards such as (ISC)², SANS, CompTIA, and (NIST) SP 800–16 are becoming prevalent in their relationship to business and industry workplace skills and therefore will remain a vital component of the curriculum development process.

Q2. What is the supply and demand situation for individuals with cyber security expertise? What evidence do you have that such individuals are in demand, and what skill sets are most in demand?

A2. As stated in previous testimony, the NSF ATE Regional Center for Systems Security and Information Assurance (CSSIA) and its partners conducted a survey of companies in five mid-western states to determine the job demand for IT security-related positions, desired skills, and preferred educational levels. The study was completed in the spring of 2004 at a regional level and shows evidence that the demand for cyber security related skills is growing. At the completion of this survey,

a total of 340 responses from companies throughout the Midwest were received. Respondents were divided into small (less than 100 employees), medium (100–499) and large (500 or more) companies. An overwhelming 99 percent of respondents were concerned about Internet and computer security. Almost three-fourths of respondents said their company currently employed people in IT security positions and IT security positions were more likely to be part-time or shared positions (part-time security along with other IT duties) than dedicated (full-time IT security). Table 1 below shows employment projections based on these 340 responses.

Additional summarized responses are as follows:

- A total of 340 responses were received. Respondents were divided into small (less than 100 employees), medium (100–499) and large (500 or more) companies.
- Almost all respondents were concerned about Internet and computer security.
- Almost three-fourths of respondents said their company currently employed people in IT security positions.
- IT security positions were more likely to be part-time or shared positions (part-time security along with other IT duties) than dedicated (full-time IT security).
- Part-time security responsibilities can be or are being added to most IT areas, including network administrator, help desk, network engineer, applications developer and systems analyst.
- Associate's degree graduates will be able to find IT security positions, both at the entry-level and experienced level, but Bachelor's degree graduates are preferred.
- The most popular types of security training provided for IT staff were self-study and commercial vendor training site. Somewhat more than two out of ten used community college classes.
- Respondents indicated a total of 166 current openings for IT security positions, and projected more openings in one year (N = 237) and still more in three years (N = 422).
- One-fourth of respondents said their company would be hiring new IT security staff within the next year. Slightly more than half said there was shortage in the current supply of qualified applicants for entry-level IT security positions. Large companies were more likely to be concerned about Internet and computer security, to have security positions, to have dedicated (that is, full-time) security positions, and to require a Bachelor's degree than medium and small companies. More than half of respondents indicated some interest in participating in IT security activities such as serving on an advisory committee, acting as an internship site, providing work-site tours, or other partnering activities.

Answers to Post-Hearing Questions

Responses by Sydney Rogers, Principal Investigator, Advanced Technology Education Regional Center for Information Technology, Nashville State Community College

Questions submitted by Representative Bart Gordon

Q1. In general, what is the state of credentialing for cyber security professionals?

Q1a. Are there certification standards in place or under development for cyber security education and training programs?

A1a. Certification standards for information security professionals have been developed by the National Security Agency (NSA) and the Committee on National Security Systems (CNSS). These standards have been incorporated into the Information Systems Security Professional certification offered by CISCO Systems. Many other organizations offer certification programs in information security. Although I do not know for sure, I assume they also incorporate the NSA and CNSS standards.

Q1b. Do formal mechanisms exist to develop such standards, and if so, please describe how they work?

A1b. I am not qualified to answer this question; however, I assume the information is available from the NSA and the CNSS. I have included a URL that provides information about those who are working on this problem.
  http://www.nsa.gov/ia/academia/

Q1c. To what extent are academic credits for cyber security studies earned though programs at one institution transferable to another in furtherance of meeting degree requirements?

A1c. In Tennessee, credits for cyber security studies will transfer from one higher education institution to another to the same degree that all other technical and courses in a specific discipline transfer. At Nashville State Community College, students may be awarded college credit toward a degree in computer networking for non-credit certification courses in cyber security and those credits will transfer to university programs that are of like disciplines. At this time in Tennessee, these credits are primarily for individual courses that are a part of degree programs in networking and telecommunications rather than for an entire degree in cyber security.

Q1d. Is there a federal role in establishing national accreditation of cyber security education and training programs, and if so, how would you characterize it?

A1d. From my perspective at the community college, it seems that accreditation standards for cyber security programs are being established by the commercial community and training programs and is widely available. If there is a federal role, I think it would be to provide a coordination or leadership function to actually get these programs implemented and get students enrolled. For instance, information coming to the college must be sought out by the college and although my college does this to some degree, many colleges do not. Too, most experts agree that for the country to achieve the best outcome, all programs must include some elements of cyber security training. If this is to happen, a proactive national effort to disseminate information and materials about the subject to community colleges, universities, and State and local school systems will be necessary. A suggested approach might be to have an office within the Department of Homeland Security with a function to coordinate all the information being developed about cyber security through NSF, NSA, and other departments and proactively organize distribution of those resources and the need to implement the programs all across the country to colleges and local school systems.

Q2. What is the supply and demand situation for individuals with cyber security expertise? What evidence do you have that such individuals are in demand, and what skill sets are most in demand?

A2. At my college, we have seen little demand for workers with specific expertise in cyber security. Instead, we have seen increased demand for network technicians and the job listings specify security knowledge as a part of the overall job description. Listings include knowledge and skills in firewall protection, knowledge of virus software, etc. In one case, an advisory committee for the health industry asked for all employees to have some understanding of cyber security and we have heard from other employers that they would like to see the curricula of all programs include elements of cyber security education to varying degrees. We have seen an increase

in the number of requests for network technicians during the last quarter. From March to May of this year we had 16 requests for such technicians and from June through August, we had 24 requests for the same job title. Most of these employers assume that the network technicians have specific knowledge of cyber security.