Homeland Security: A Technology Forecast

Authored by:
John Vanston, Ph.D.
&
Henry Elliott, M.S.M.E.

Program Director:
Michael Bettersworth, M.A.
### Table of Contents

- List of Appendices .......................................................... vi
- List of Figures ................................................................... vii
- List of Tables ..................................................................... vii
- Preface ............................................................................... viii
- Acknowledgments ................................................................ ix
- Executive Summary .......................................................... 1
  - Role of Texas Community and Technical Colleges .......... 1
  - Purpose of This Report .................................................... 1
  - Evaluating Potential HS Programs ................................. 1
  - Final Analysis .................................................................. 2
  - Background ..................................................................... 3
- General Observations .......................................................... 5
  - Key Players ...................................................................... 5
  - Level of Effort .................................................................. 5
  - Government Guidance .................................................... 5
  - Commercial Involvement ............................................... 5
  - Coordination Difficulties ............................................... 6
  - Federal Government Programs ....................................... 6
  - Texas Government Programs ......................................... 6
- Workforce Implications .......................................................... 9
  - Increasing Opportunities ............................................... 9
  - Small Business Opportunities .......................................... 9
  - Employment Categories .................................................. 9
- Community and Technical College Homeland Security Strategies ........................................... 11
  - Community and Technical College Goals ....................... 11
  - Approaches ..................................................................... 11
  - Special Considerations ................................................... 12
  - Attractiveness of HS Specialist Areas .............................. 12
  - Employment Opportunities ............................................ 13
  - Compatibility with Current Curricula .............................. 14
  - Overall Attractiveness ................................................... 14
  - Specialist Category Attractiveness ................................... 14
- Identification ..................................................................... 15
  - Job Title ......................................................................... 15
  - Job Responsibilities ........................................................ 15
  - Required Knowledge, Skills, and Abilities ....................... 15
  - Extra Desired Knowledge, Skills, and Abilities ................ 15
  - Driving Forces for Employment ....................................... 15
  - Ratings ........................................................................... 16
  - Opportunity Timing ........................................................ 17
  - Special Texas Factors ...................................................... 17
  - Special Instructor Requirements ..................................... 18
  - Special Equipment Requirements .................................... 19

---

**HOMELAND SECURITY A TECHNOLOGY FORECAST >> SEPTEMBER 2004**

---
Network Security ........................................................................................................................................... 21
Job Title ...................................................................................................................................................... 21
Job Responsibilities ....................................................................................................................................... 21
Required Knowledge, Skills, and Abilities ................................................................................................. 21
Driving Forces for Employment .................................................................................................................. 21
Special Texas Factors ................................................................................................................................ 22
Ratings ......................................................................................................................................................... 22
Opportunity Timing ...................................................................................................................................... 23
Special Instructor Requirements .................................................................................................................. 25

Weapons of Mass Destruction Detection ................................................................................................ 27
Job Title ...................................................................................................................................................... 27
Job Responsibilities ....................................................................................................................................... 27
Required Knowledge, Skills, and Abilities ................................................................................................. 27
Driving Forces for Employment .................................................................................................................. 27
Ratings ......................................................................................................................................................... 28
Special Instructor Requirements .................................................................................................................. 29

Weapons of Mass Destruction Mitigation/Decontamination ................................................................. 31
Job Title ...................................................................................................................................................... 31
Job Responsibilities ....................................................................................................................................... 31
Required Knowledge, Skills, and Abilities ................................................................................................. 31
Driving Forces for Employment .................................................................................................................. 31
Ratings ......................................................................................................................................................... 31

Concealed Explosives .................................................................................................................................... 33
Job Title ...................................................................................................................................................... 33
Job Responsibilities ....................................................................................................................................... 33
Required Knowledge, Skills, and Abilities ................................................................................................. 33
Driving Forces for Employment .................................................................................................................. 33
Special Texas Factors ................................................................................................................................ 34
Ratings ......................................................................................................................................................... 35

Critical Infrastructure Security .................................................................................................................. 37
Job Title ...................................................................................................................................................... 37
Job Responsibilities ....................................................................................................................................... 37
Required Knowledge, Skills, and Abilities ................................................................................................. 37
Driving Forces for Employment .................................................................................................................. 37
Ratings ......................................................................................................................................................... 38

Pattern Analysis ............................................................................................................................................ 41
Job Title ...................................................................................................................................................... 41
Job Responsibilities ....................................................................................................................................... 41
Required Knowledge, Skills, and Abilities ................................................................................................. 41
Driving Forces for Employment .................................................................................................................. 41
Ratings ......................................................................................................................................................... 42

Current and Developing Educational Projects .......................................................................................... 45
Federal Programs ........................................................................................................................................ 45
Private and College Programs .................................................................................................................... 45
Other Programs .......................................................................................................................................... 50
### Part 2: Technologies Associated with Homeland Security Programs

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>55</td>
</tr>
<tr>
<td>General</td>
<td>55</td>
</tr>
<tr>
<td>Biometric Technologies</td>
<td>56</td>
</tr>
<tr>
<td>Physiological Characteristics</td>
<td>56</td>
</tr>
<tr>
<td>Behavioral Characteristics</td>
<td>61</td>
</tr>
<tr>
<td>Commercial Off-the-Shelf Status of Biometric Technologies</td>
<td>63</td>
</tr>
<tr>
<td>Dynamic Growth</td>
<td>63</td>
</tr>
<tr>
<td>Biometrics Industry and Technology Trends</td>
<td>67</td>
</tr>
<tr>
<td>Industry Trends</td>
<td>67</td>
</tr>
<tr>
<td>Technology Trends</td>
<td>68</td>
</tr>
<tr>
<td>Weapons of Mass Destruction Detection</td>
<td>71</td>
</tr>
<tr>
<td>General</td>
<td>71</td>
</tr>
<tr>
<td>Chemical Detection Technologies</td>
<td>71</td>
</tr>
<tr>
<td>Technical Underpinnings</td>
<td>76</td>
</tr>
<tr>
<td>Biological Detection Technologies</td>
<td>77</td>
</tr>
<tr>
<td>Nuclear Weapons</td>
<td>78</td>
</tr>
<tr>
<td>Weapons of Mass Mitigation and Decontamination</td>
<td>79</td>
</tr>
<tr>
<td>General</td>
<td>79</td>
</tr>
<tr>
<td>Federal Standards</td>
<td>79</td>
</tr>
<tr>
<td>Overview of Chemical-Biological Decontamination</td>
<td>79</td>
</tr>
<tr>
<td>Network Security</td>
<td>85</td>
</tr>
<tr>
<td>Background</td>
<td>85</td>
</tr>
<tr>
<td>Decreasing a Network’s Vulnerability to Attack</td>
<td>86</td>
</tr>
<tr>
<td>The Layered-Security Model</td>
<td>86</td>
</tr>
<tr>
<td>Concealed Explosives</td>
<td>91</td>
</tr>
<tr>
<td>Background</td>
<td>91</td>
</tr>
<tr>
<td>X-ray Based Technologies</td>
<td>91</td>
</tr>
<tr>
<td>Neutron Transmission Based Technologies</td>
<td>93</td>
</tr>
<tr>
<td>Tracing Molecules Of Explosive Materials</td>
<td>95</td>
</tr>
<tr>
<td>Next Generation</td>
<td>96</td>
</tr>
<tr>
<td>Critical Infrastructure Security</td>
<td>97</td>
</tr>
<tr>
<td>Background</td>
<td>97</td>
</tr>
<tr>
<td>Peripheral Security</td>
<td>97</td>
</tr>
<tr>
<td>Access Control and Internal Security</td>
<td>99</td>
</tr>
<tr>
<td>Multi-Level Detection Systems (Weapons and Explosives)</td>
<td>100</td>
</tr>
<tr>
<td>Pattern Analysis</td>
<td>103</td>
</tr>
<tr>
<td>Background</td>
<td>103</td>
</tr>
<tr>
<td>Data Warehousing</td>
<td>103</td>
</tr>
<tr>
<td>Data Mining</td>
<td>104</td>
</tr>
<tr>
<td>“Distributed” Data Mining</td>
<td>105</td>
</tr>
<tr>
<td>Information Sharing</td>
<td>106</td>
</tr>
<tr>
<td>Link Analysis</td>
<td>106</td>
</tr>
<tr>
<td>Text Mining</td>
<td>107</td>
</tr>
<tr>
<td>Phenomenal Data Mining</td>
<td>108</td>
</tr>
<tr>
<td>Spatial and Geographic Data Mining</td>
<td>108</td>
</tr>
</tbody>
</table>
Table 1
Summary of Factors Relevant to Colleges in Implementing Programs ........................................... 2
Table 2
Colleges with Awards in Network Security Technology ................................................................. 23
Table 3
Explosive Specialist Tasks ............................................................................................................. 33
Table 4
TSTC Waco Medical Imaging Systems Technology Curriculum .................................................. 36
Table 5
The Protection Challenge .................................................................................................................. 39
Table 6
Critical Infrastructure Tasks .............................................................................................................. 40
Table 7
Chemical Detectors ........................................................................................................................ 72
Table 8
Estimated Human Exposure Guidance for Selected Chemical Warfare Agents ......................... 74
Table 9
Technologies Used in Chemical Weapon Detection ...................................................................... 76
Table 10
Levels of Security ........................................................................................................................... 86
The research presented in this report is designed to provide Texas community and technical college instructional officers and curriculum development coordinators/directors with timely analysis and actionable insights into emerging technologies and their potential impacts on existing and new technical education curricula. A highly-skilled workforce is essential to the success of Texas companies and the overall economic competitiveness of the state. Therefore, by anticipating and proactively responding to future Texas workforce demands, community and technical college curriculum offerings can be a constructive force in attracting high-tech companies to the state and ensuring existing high-tech companies continue to have an appropriately skilled source of employees. Through this research, TSTC hopes to drive the development and support of emerging technology curricula and facilitate informed and accurate future curriculum development efforts for all Texas community and technical colleges.
Although there is a great interest throughout the country in Homeland Security (HS) issues and a commitment to developing an effective HS program, in reality there is little clear public understanding about the precise meaning of the term or appreciation of what must be done to insure the security of the nation and its citizens. Although a number of government publications are now available, in a situation such as exists today, both information and wisdom depends, in large measure, on personal contacts with people who are currently involved in HS activities. In developing this report, the authors have been impressed with the competence and commitment of HS professionals with whom we have interacted and we are extremely grateful to them for the advice, information, and insights, that they have provided.

Although there are many people who have assisted us in the preparation of this report, the authors would like to give special thanks to the following people:

**Steve Cooperman**, Vice President, Oracle Homeland Security Solutions, for providing information about the Information Management challenges the government faces in ensuring Homeland Security.

**Jim Wrightson**, Vice President of Homeland Security, Lockheed-Martin, for providing information about the role of large scale system integrators (DoD contractors) in Department of Homeland Security port security, critical infrastructure and pattern analysis (data mining) initiatives.

**Rex Richardson**, Chief Scientist, SAIC Cargo Inspection Operation-San Diego, for providing information about the training requirements and employment opportunities for cargo and baggage inspection systems technicians.

**Glen McNeil**, Senior Director of Strategic Engineering, SAGEM Morpho, Inc., for providing information about federally mandated biometric initiatives and employment opportunities for technical and community college graduates in the biometrics area.

**Lori Bush**, Senior Adviser, Cisco Homeland Security Group, for providing information about security issues related to networking in government information technology domains.


**Jack Colley**, Texas State Coordinator, Governor’s Division of Emergency Management-Department of Public Safety, for providing information about the role of DPS in State Homeland Security activities.

**Retired Major General Todd Stewart**, Director, Program for International and Homeland Security at Ohio State University and also Executive Director, National Academic Consortium for Homeland Security, for providing information on academic institutions (2 year and 4 year) offering Homeland Security programs.

**M. Paul Collier**, Executive Director, The Biometric Foundation, for providing background information on the use of biometrics in commercial, government, and military applications.

**Dr. Melissa Stark**, Assistant Director for Educational Programs, Purdue Center for Education and Research in Information Assurance and Security, for providing an overview of continuing education programs for the Center for Education and Research in Information Assurance and Security at Purdue University.
Dr. Walter McCollum, Biometrics Education Program Manager, Department of Defense Biometrics Management Office, for providing an overview of the Army’s Graduate Certificate Program in Information Assurance and Biometrics that will be offered through the College of Engineering and Mineral Resources at the University of West Virginia.

Gerald Adams, former Senior Advisor to Deputy Attorney General of Texas, Jay Kimbrough, for providing an overview of the Texas Department of Homeland Security and its interaction with the 22 Council of Governments and Regional Councils.

Robert Weaver, Deputy Special Agent in Charge N.Y. Electronic Crimes Task Force, United States Secret Service, for providing an overview of the Secret Service’s approach to conducting vulnerability assessments and Homeland Security in the Information Assurance arena.

Dr. Robert Krienke, President, Lamar Institute of Technology, for his guidance and unwavering support in the development of the Texas Center for Homeland Security Training at the Institute.

Sam Williams, Vice President for Academic Affairs, Lamar Institute of Technology, for providing an overview of the activities of the Texas Homeland Security Consortia.

Jim Doane, Director of Homeland Security and Criminal Justice Training, Lamar Institute of Technology, for providing an overview of the Homeland Security curriculum at the Lamar Institute of Technology.

Mel Mireles, Director, Enterprise Operations Division, Texas Department of Information Resources, for providing an overview of his office’s role in Homeland Security and possible employment opportunities for residents of the State.

In addition, we would like to thank William Cisario, Jack Peregrim, and Barbara Heimlich of Paragon Development for inviting one of the authors to participate in a forum examining the commercial opportunities afforded by various government Homeland Security programs. We would also like to thank the other participants in this forum who provided a great numbers of insights about current and planned government HS activities. These participants included:

Joseph Smith, Vice President Applied Research Associates, Inc.
Michael Hunt, MD, Emergency Medical Specialist, CarePoint, P.C.
James Ball, President, Ball & Associates, Inc.
James Litchko, President, Litchco & Associates, Inc.
Paul Pattak, President, The Byron Group, Ltd.

A very special debt of gratitude is owed to Michael Bettersworth, Associate Vice Chancellor for Technology Advancement, Texas State Technical College Systems Operations Office, who obtained funding to support this research, provided expert guidance, arranged important meetings, and, above all, spent an unknown number of hours editing this report.

No project of this type is possible without funding support. In this case the authors would like to particularly thank, Robert Franks, Director of Perkins Grants Administration, Texas Higher Education Coordinating Board, for authorizing a Carl D. Perkins grant to support this project. Mr. Franks has shown a keen understanding of the purpose and value of analyses of this type.
Finally, the authors would like to thank: Charlene Canaris and Carmen Keiningham, Administrative Assistants, Texas State Technical College System Operations, for helping arrange interviews, travel, and required reporting; Debbie Moore, Prepress Technician I, Printing Production, Texas State Technical College Waco, for her outstanding layout skills, final editing, and the recreation of many tables and other elements; Mark Burdine, Coordinator of Photography, Texas State Technical College Waco, for his excellent cover art and many of the images found throughout this report; Debra Robison, Administrative Director, Technology Futures, Inc., for her assistance in drafting; Eliska Beaty, Associate Vice Chancellor for Marketing and Communications, Texas State Technical College System and Jan Osburn, Director of Marketing and Communications, Texas State Technical College Waco, for their continued support of this research and expert advice; and Bill Evridge, Director of Printing Production, Texas State Technical College Waco, and TSTC Waco Printing Production for printing, duplicating, and binding this report. This report would not have been possible without the efforts of these individuals, and their skills and dedication are greatly appreciated.

The primary foundation of this technology forecast is the input that we have received from the listed experts and a number of other people with whom we interacted during the conduct of this forecast. The forecast reflects the authors' interpretations of these inputs. Any misinterpretations of these inputs are the fault of the authors, and we apologize for these to the people who have so obligingly contributed to our efforts.

John H. Vanston and Henry Elliott
The events of September 11, 2001 brought immediate attention to the challenges of internal security in the United States. The realization of these challenges resulted in a number of actions by federal, state, and local governments, including the establishment of the Department of Homeland Security (DHS).

Role of Texas Community and Technical Colleges

Because the stated policy of the Texas State government is to place primary responsibility for HS planning, training, and execution in the hands of local governments, e.g., Councils of Government (COGs) and Regional COGs, it is obvious that the experience, structure, and missions of the State’s Community and Technical Colleges make them particularly well suited for training the people needed to support the State’s Homeland Security (HS) requirements.

Fully capitalizing on these opportunities will require careful planning and prompt execution. College deans and other instructional officers must be cognizant of the emerging opportunities and appreciate how current programs can best be modified to provide the required knowledge, skills, and abilities. The objective of this report is to provide these leaders with information to assist in making informed decisions regarding the future impact of HS and the resulting potential technical workforce needs.

Purpose of This Report

This report presents information, ideas, and concepts that should be of value to College instruction officers in making reasoned decisions about the design, initiation, and conduct of HS programs in their institutions, as well as analyses of seven technology areas that provide technical underpinnings for the nation’s homeland security agenda.

Evaluating Potential HS Programs

The seven technology areas identified for analysis were:

- Identification Specialists
- Network Security Specialists
- Weapons of Mass Destruction (WMD) Detection Specialists
- WMD Mitigation and Decontamination Specialists
- Concealed Explosives Specialists
- Critical Infrastructure Security Specialists
- Pattern Analysis/Data Warehouse Specialists

In evaluating the attractiveness of College HS programs in these areas, three factors were considered:

State of Maturity

The most attractive HS specialist areas will be those that offer attractive, long-term opportunities to students.
Employment Opportunities

Employment opportunity attractiveness considers the near-term availability of attractive employment.

Compatibility with Current Curricula

Compatibility attractiveness reflects the ease with which new programs could be added to current curricula.

Overall Attractiveness

Based on these three factors, an Overall Attractiveness rating was assigned to each specialist area. Results of these evaluations are presented below.

Table 1 Summary of Factors Relevant to Colleges in Implementing Programs

<table>
<thead>
<tr>
<th>Employment Category</th>
<th>State of Maturity Rating</th>
<th>Employment Opportunities Rating</th>
<th>Current Curriculum Compatibility Rating</th>
<th>Overall Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification Specialist</td>
<td>Very Well</td>
<td>Fairly Promising</td>
<td>Somewhat Compatible</td>
<td>Somewhat Attractive</td>
</tr>
<tr>
<td>Network Security Specialists</td>
<td>Very Well/Structured</td>
<td>Very Promising</td>
<td>Very Compatible</td>
<td>Very Attractive</td>
</tr>
<tr>
<td>WMD Detection Specialists</td>
<td>Fairly Well/Structured</td>
<td>Not Very Promising</td>
<td>Very Compatible</td>
<td>Not Very Attractive</td>
</tr>
<tr>
<td>WMD Mitigation and Decontamination Specialists</td>
<td>Not Well/Structured</td>
<td>Not Very Promising</td>
<td>Not Very Compatible</td>
<td>Not Very Attractive</td>
</tr>
<tr>
<td>Concealed Explosives Specialists</td>
<td>Very Well/Structured</td>
<td>Fairly Promising</td>
<td>Somewhat Compatible</td>
<td>Somewhat Attractive</td>
</tr>
<tr>
<td>Critical Infrastructure Security Specialists</td>
<td>Very Well/Structured</td>
<td>Very Promising</td>
<td>Very Compatible</td>
<td>Very Attractive</td>
</tr>
<tr>
<td>Pattern Analysis/Data Warehouse Administration</td>
<td>Well/Structured</td>
<td>Promising</td>
<td>Quite Compatible</td>
<td>Quite Attractive</td>
</tr>
</tbody>
</table>

Final Analysis

Overall, the increasing importance of homeland security, the expansion of security needs, and the rapidly growing level of funding for security products and services offer a dramatic opportunity for the Texas Colleges to fulfill their missions of contributing to the well being of the State and providing attractive employment opportunities for their graduates.
Background

The events of September 11, 2001 brought immediate attention to the challenges of internal security in the United States. The realization of these challenges resulted in a number of actions by federal, state, and local governments, including the establishment of the Department of Homeland Security (DHS) www.dhs.gov. This department has been organized to address four different areas of concern:

- Border and Transportation Security.
- Emergency Preparedness and Response.
- Chemical, Biological, Radiological and Nuclear Countermeasures.
- Information Analysis and Infrastructure Protection.

Although each of these areas involve factors other than technology, it is obvious that a wide range of technologies will be required to accomplish the nation’s objectives in each of these areas. It is also obvious that there will be many technologies that will be applicable in more than one area. The variety of technologies involved in homeland security will enhance the probability of attractive employment for community and technical college graduates.

In the opinion of many, development of procedures, training and operations standards, and required technology, as well as allocation of appropriate funding has been agonizingly slow. However, recently, there has been significant progress in all of these areas. The increased importance of homeland security, the expansion of security needs, and the rapidly growing level of funding for security products and services offer a dramatic opportunity for the community and technical colleges of Texas.

No other group is as well prepared by organization, experience, and tradition to provide trained technicians in a timely and expeditious manner than the Texas community and technical colleges. As Secretary of Labor Elizabeth Chao stated in an address to the American Association of Community Colleges in February of 2002, “No one is doing better than you [community colleges] when it comes to preparing workers for 21st century jobs...Homeland Security is, sadly, the latest in need of thousands of highly skilled workers. We can’t seem to work fast enough to increase and improve the security of our workplaces, transportation systems, borders, and ports.”1 The establishment of appropriate Homeland Security (HS) programs will not only support the development of very attractive employment opportunities for Texas community and technical college graduates, but will also enhance the economic well being of the State and contribute to the continuing safety and security of the nation.

Although the employment opportunities in the HS area will be extensive, fully capitalizing on these opportunities will require careful planning and prompt execution. College deans and other instructional officers must be cognizant of the emerging opportunities and appreciate how current programs can best be modified to provide the required knowledge, skills, and abilities. The objective of this report is to provide these leaders with information to assist in making informed decisions regarding the future impact of HS and the resulting potential technical workforce needs.

This report is organized in two parts. Part One presents information, ideas, and concepts that should be of value to college instructional officers in making reasoned decisions about the design, initiation, and conduct of HS programs in their institutions. Part Two presents analyses

---

of seven technology areas that provide technical underpinnings for the nation’s homeland security agenda and is designed to provide college instructional officers with more detailed information about each technology to assist in the HS decision process. Following these two parts there is a Final Comments section that summaries the material presented in both parts of the report.

Part one of the report is organized into five sections as follows:

- General Observations
- Workforce Implications
- Suggested College HS Strategies
- Attractiveness of HS Specialist Areas
- Current and Developing Education Programs

Although many non-technology HS jobs, such as administrative, clerical, and financial positions, will become available because of the expansion of homeland security activities, it is believed that the knowledge, skills, and abilities (KSAs) required for these new and evolving jobs will be little different from similar jobs now available in other non-related fields. Therefore, this report will focus on technology-related employment jobs.
Key Players

There will be two basic players addressing the HS needs of the nation-government and commercial sectors. The federal government will play a key role in defining needs, establishing standards, and enforcing compliance, and will provide considerable funding. However, the bulk of HS responsibilities, activities, and funding will fall under the aegis of the nation’s commercial sector.

Level of Effort

Although there has been considerable discussion about the need for enhanced security, the number of regulations promulgated and the amount of money appropriated by the government and committed by commercial organizations has, to date, been relatively small. However, actions by the federal government appear to be increasing, including the development of compliance standards and the allocation of HS funding. However, many individuals and organizations have indicated that the amount of money allocated to date is much too small.

Government Guidance

Government dissemination of regulations and standards has, to date been spotty. Individual identification requirements have been well defined in the Aviation and Transportation Security Act, the Transportation Workers Identification Card program, and the Patriot Act. In addition, the Department of Justice, through its National Institute of Justice (NIJ) program, has recently released a series of chemical and biological equipment guides that focus on the areas of detection, personal protection, decontamination, and communications. On the other hand, guidance is currently limited in a number of important HS areas such as critical infrastructure protection and intelligence gathering (pattern analysis).2

Commercial Involvement

For the commercial sector, many of the industries (e.g. petroleum refineries, chemical plants, and railroad terminals) most vulnerable to terrorist attack have been very reluctant to take needed action because of the costs involved. In most cases, only limited commitment to new HS procedures can be expected until government incentives, either through financial support or new regulations, are provided. There is little doubt that such incentives will be forthcoming. However, there is no certainty about the timing of such incentives or resulting employment opportunities.

---

Coordination Difficulties

Many of the companies with interest in HS issues have found it difficult to interact effectively with the DHS because:

- “The money trail is difficult to follow.
- Acquisition offices are “immature” because of drawn-out procurements and the integration of multiple agencies.
- Congressional oversight committees are not completely functional, leaving industry feeling homeless.
- Large prime contractors serve as marketing conduits for smaller, niche firms.
- There is lack of indemnification from unlimited liability if a solution fails.”

Federal Government Programs

A number of federal programs will have an impact on HS. Areas of impact include port security, aviation security, urban security and regional first responders, US Visitor and Immigrant Status Technology (VISIT), and information analysis and infrastructure protection. A detailed description of major federal HS programs is provided in Appendix A.

Texas Government Programs

Texas House Bill 9

Texas House Bill 9 gives the governor the duty of organizing and directing State HS strategies and initiatives. The Bill also gives the governor the power to allocate and review HS grants and funding levels and to administer an interagency advisory group called the Critical Infrastructure Protection Council, which includes representatives from these State agencies: the Department of Agriculture, the Office of the Attorney General, the General Land Office, the Public Utility Commission, the Texas Department of Health, Department of Information Resources, Department of Public Safety, Division of Emergency Management of the office of the Governor, Texas National Guard, Texas Commission on Environmental Quality, Railroad Commission, Texas Strategic Military Planning Commission, and Texas Department of Transportation.

Under House Bill 9, the DPS is recognized as the depository for intelligence information related to HS activities. Additionally, the bill requires pharmacists to report “unusual incidents or trends that might suggest bioterrorism or serious disease outbreaks and adds emergency medical service personnel, peace officers, and firefighters to those required to report suspected cases of reportable diseases.” The Bill also creates confidentiality provisions related to information about critical infrastructure, information technology architectures and implementations, tactical plans, vulnerability assessments, and contact numbers for emergency first responders. A detailed description of major state HS programs is provided in Appendix B.

---

4,5 Texas House Bill 9. www.tlc.state.tx.us/research/78soe/5035.htm
Texas Homeland Security Organization

Mr. Steven McCraw is the Director of Homeland Security for Texas, and Mr. Jay Kimbrough is the Senior HS Advisor to Governor Perry. A basic principle of the State’s HS program is regionalism, i.e., local control. Each of the State’s 254 counties belongs to one of the State’s 22 Councils of Government (COGs), and the number of counties per COG varies from three to 22. Each of these 22 COGs are, in turn, organized into 10 Regional Councils (RCs).

Each COG is composed of leaders familiar with the infrastructure within its boundaries, and, therefore, the COGs and the RCs are better suited to conduct terrorism vulnerability assessments than the State Government. The Texas Engineering Extension Service relies on the vulnerability assessments developed by the COGs and RCs to allocate the funds it distributes under the Domestic Preparedness program. An important function of McCraw’s office is to know which councils of government are able to assist adjoining COGs with resources or manpower. The office also must know what resources may be available from those COGs, since every region needs to have the equipment to detect, deter and respond to a mass disaster. This information will be very important in the event of an attack because it would assist in getting resources to an event quickly, saving lives and properties. The response to an attack would be managed by the Department of Public Safety’s Division of Emergency Management at its Texas Security Alert and Analysis Center, which is located in Austin at a facility 30 feet underground. Jack Colley is the State Coordinator of the Governor’s Division of Emergency Management within the DPS.

Recent State HS Grant

On May 20, 2004 Governor Rick Perry announced that 544 Texas jurisdictions would receive $54 million dollars in 2004 First Responder Equipment Grants from the Office of Domestic Preparedness (ODP). These grants, which are awarded based on an assessment of threat and vulnerability prepared by each jurisdiction, allow for the purchase of decontamination equipment, hazmat suits and other equipment to support their regional response plans. The Texas Engineering Extension Service (TEEX), under the direction of Charlie Todd, is the State Administrative Agency for the Domestic Preparedness program. TEEX uses the vulnerability assessments to prioritize jurisdictions and allocate funding. All counties and cities in Texas are eligible to submit an assessment and receive funding. 6

Increasing Opportunities

Although government funding to date has been limited, there are strong indications that the level of funding will be rising steadily over the next few years. For example, the DHS Budget for FY 2004, $37.6 billion dollars, was 11 percent more than the 2003 level. Additionally, DHS recently announced the awarding of the $10 billion dollar US Visitor and Immigrant Status Indicator Technology (VISIT) project, which will track the entry and exit of non-US citizens into and out of the US. Moreover, as the reorganization of DHS continues, new regulations will require significant expansion of commercial funding of HS activities. In short, there are currently attractive employment opportunities in the HS area, and there is little doubt that these opportunities will grow dramatically in the future. Moreover, these opportunities will remain intact for the foreseeable future since it appears that the basic threat will continue. However, the timing of these expected employment opportunities is uncertain and will vary between the different government and commercial sectors.

Small Business Opportunities

Although details of the federal and state government HS programs, as well as related commercial programs, are not well defined at this time, for many of these programs, both government and commercial entities will probably prefer to utilize large established companies as prime contractors (e.g., Accenture’s role in US VISIT program) to insure that proper standards are maintained. However, because of the distributed nature of many of these programs, there is a good possibility that these prime contractors will subcontract with smaller companies for the actual conduct of the work. This approach would be similar to common practices in areas such as construction, appliance repair, and service activities, and would provide many opportunities for community and technical college graduates.

Employment Categories

The release of requests for new products and services (www.bids.tswg.gov/hsarpa) provides indications of the type of new technologies and services that will be required by the DHS. An examination of these requirements, plus the federal and state government activities described above provides a basis for identifying the types of technicians that will be required by the HS community. The types of technicians required can be classified into seven specialty areas:

- Identification
- Network Security
- Chemical, Biological, and Nuclear (CBN) Detection
- CBN Mitigation and Decontamination
- Concealed Explosives
- Critical Infrastructure Security
- Pattern Analysis/Data Warehouse Administrator

Technologies involved in each of these areas are described in Part II of this report.
The challenge facing the Deans and other community and technical college instructional officers is how to translate the information and ideas presented in the previous sections and Part II of this report into programs that will provide graduates of the institutions with attractive employment opportunities. Although the situation will be different in each college, the following comments are intended to assist them in meeting this challenge.

Community and Technical College Goals

At this time, it appears that the most appropriate goal for community and technical colleges is to create separate programs in specialty areas that they believe offer attractive employment opportunities for their graduates. Within each of the chosen specialty areas, colleges should train their students in all of the key technologies involved in that area. For example, network security technicians should be trained to perform computer network vulnerability assessments and install, configure, and maintain a wide variety of network security products including internal and external security firewalls. They should understand the technical principles involved in encryption and virtual private networks. They should also be trained to perform network security audits to ensure that there have been no successful breaches of security. This foundation should prepare them to become valuable members of network security teams.

Because of the large amount of knowledge, skill, and abilities required in each category, the training of individuals in multiple HS categories would be difficult and, probably, counterproductive.

Approaches

Three approaches are available to community and technical colleges in the area of HS programs:

- Substitute or add one or two HS-related courses into a current program.
- Initiate HS-related Level II or Advanced Training Certificate programs for current students and former graduates.
- Initiate an Associate Degree in Homeland Security.

Obviously, any college can follow more than one strategy, and often they may be combined. For example, a given course might be included in all of the three approaches. Such combination might be very useful in regard to effective utilization of special equipment and qualified faculty.

The Substitution in Current Program approach will be the easiest to implement. In most cases, students involved in this approach will not receive any formal recognition of their HS training. However, in applying for HS-related employment, the fact that they have been explicitly trained in a particular HS technology may increase their employment status. In some cases, the HS-related courses may allow professional certification such as Certified Oracle Database Administrator. However, program planners must take care that the substitutions do not impact the students’ qualifications in the primary areas of their degrees.

The Initiate Level II or Advanced Training Certificate Program approach probably provides the most attractive short-term alternative. The three or six month extra training provided will allow current students to continue with their present programs until completion and then acquire HS-related KSAs required for successful employment in one or more HS technology areas. These programs will allow former college graduates to add market attractive capabilities to their previous qualifications. In most cases, it will be possible to organize programs that will support formal certification in the appropriate areas.
The Initiate an Associate Degree Program in Homeland Security approach probably offers the most appropriate long-term alternative. In this regard, community and technical colleges may find it useful to coordinate development efforts among themselves through the Nationwide Homeland Security Curriculum Development Consortium, which the Lamar Institute of Technology in Beaumont has been very active in leading. When curricula developed by the Consortium are certified, they can be adopted and initiated with little administrative effort. The Consortium will conduct a National Homeland Security DACUM September 17-19, 2004 at the Houston Bush International Airport Marriott.

However, many colleges may wish to develop new programs that are more appropriate to their local situations. In these cases, colleges will, of course, have to receive approval for the program using the procedures outlined in Guidelines for Instructional Programs in Workforce Employment (GIPWE). Due to the broad nature of HS technologies and likely differences in curriculum needs, it may also be necessary to form additional consortia specific to one or more of the seven technical areas previously listed.

**Special Considerations**

**Scope**

Because of the wide diversity of technologies involved in HS, instructors will probably have to concentrate their courses in a single technology area and, perhaps, on only a selected part of that area. In technology areas expanding as rapidly as the ones addressed in this report, it is also important that the curriculum and lab space remain up-to-date with the latest technologies.

**Coordination**

As described in the following section, many government agencies, educational institutions, and commercial organizations have developed or are developing HS training and instructional programs ranging from those offering bachelor degrees to half-day sessions. In utilizing any of the three approaches described above, these programs can serve as models for colleges. Consideration should also be given to coordinating HS programs with similar programs at neighboring four-year universities (e.g. CIAS at UTSA).

**Attractiveness of HS Specialist Areas**

**General**

In the Workforce Implications section of this report, seven specialty areas of HS were identified. In this section, each of these specialist areas are analyzed in terms of the state of maturity of the underlying technology areas, potential employment opportunities, compatibility with current college programs, and overall attractiveness for adoption by the community and technical colleges throughout the State. Each category is given a qualitative rating in each of these areas. Although these ratings are, to a considerable extent, subjective, they are all supported by extensive literature searches and discussions with respected subject matter experts. (A partial listing of literature sources is presented in Appendix C and a partial listing of experts consulted during this project is presented in Appendix D). It should be noted that these ratings apply to the college community as a whole and may not be relevant to individual colleges, because local needs may differ.
State of Maturity

The state of maturity of the technologies on which the employment categories are based is important in evaluating their attractiveness to colleges. These states can be classified into three types.

- Mature technologies, such as database administration, are those that have been available for a considerable period of time, are fully developed, and promise limited probability of future change. Programs for training technicians in these areas are currently available in some cases and graduates trained in these technologies may or may not profit from unique job qualification.

- Emerging technologies that are currently available, but have not achieved widespread adoption, such as real-time data warehouses, will offer college graduates increasing employment opportunities as they become increasingly prevalent.

- Forefront technologies that are still in the early development stage, such as dynamic typing identification, will not be attractive because employment opportunities will be limited in the foreseeable future.

The most attractive HS employment areas will be those that offer a mixture of technical maturities with a particularly large fraction occurring in the emerging technology area. The existence of mature technologies in a specialty area increases the probability that jobs will be available immediately on graduation; the existence of emerging technology areas increases the probability of near-term attractive employment; and the existence of forefront technology areas increases the probability that attractive employment in the area will remain strong for a long period of time. In this section, the following scheme will be used to rate each specialist area in terms of its state of maturity attractiveness.

**Very Well Structured:** Some technologies in both the mature and forefront areas with a very significant number of technologies in the emerging area.

**Well Structured:** A significant number of technologies in the emerging area, but few or none in the mature or forefront areas.

**Fairly Well Structured:** Technologies equally divided between the mature, emerging, and forefront areas or between the emerging area and either of the other two areas.

**Poorly Structured:** Most technologies in either the mature or forefront areas.

Employment Opportunities

Obviously, one of the most important factors to be considered in evaluating the attractiveness of the various specialist areas is the opportunity for employment in the area. This evaluation will consider the total number of technicians that will be required both statewide and nationwide, how long it will take the projected jobs to materialize, the types of jobs involved, and salary levels for these jobs. The rating scheme to be used for this factor is as follows:

**Very Promising:** A large number of well paying, attractive jobs will be available almost immediately, and this number will continue to grow for the foreseeable future.

**Promising:** A significant number of reasonably well paying jobs will be available in the near future, and the number will continue to grow for the several years.

**Fairly Promising:** A limited number of fairly well paying jobs will be available in the not too distant future, and this number will stay effectively even for the next few years.

**Not Very Promising:** A small number of jobs of limited attractiveness will be available for a few years.
Compatibility with Current Curricula

Another important factor in determining the attractiveness of each employment category is the ease with which currently available curricula can be modified and expanded to provide graduates with the KSAs required for successful employment in that area of technology. This evaluation will include consideration of special equipment and qualified faculty requirements. The rating scheme to be used for this factor is as follows:

**Very Compatible:** Programs providing the required KSAs will be quite similar to current programs currently being offered at a large number of colleges.

**Quite Compatible:** Programs providing the required KSAs will be rather similar to current programs currently being offered at a fair number of colleges.

**Somewhat Compatible:** Programs providing the required KSAs will be moderately similar to current programs currently being offered at a small number of colleges.

**Not Very Compatible:** Few programs currently being offered at any colleges will be at all similar to current programs.

Overall Attractiveness

Once attractiveness ratings have been assigned to each of these three factors, these ratings must be considered in concert to determine an “Overall Attractiveness” rating. The rating scheme to be used for this synthesis is as follows:

**Very Attractive:** Initiation of programs in this employment category will be very attractive to a large number of colleges.

**Quite Attractive:** Initiation of programs in this employment category will be quite attractive to a medium number of colleges.

**Somewhat Attractive:** Initiation of programs in this employment category will be somewhat attractive to a small number of colleges.

**Not Very Attractive:** Initiation of programs in this employment category will be of limited attractiveness to only a small number of colleges.

Specialist Category Attractiveness

The following sections discuss the level of attractiveness associated with initiating community and technical college programs in the seven previously identified HS specialist areas.
Job Title

Biometrics Systems Specialist
Systems Technician

Job Responsibilities

Biometrics Systems Specialists will have the ability to enroll subjects into a biometrics system by capturing a sample of one or more unique personal characteristics (physiological or behavioral) and then processing the sample to produce a reference for the individual concerned. The Specialist will also interact with Information Technology (IT) systems that contain stored samples to verify information and/or confirm the identity of the enrollee.

Biometrics Systems Technicians will have the ability to install, calibrate, maintain, and repair one or more kinds of biometrics systems.

Required Knowledge, Skills, and Abilities

- Understand the basic principles of biometric identification processes.
- Be able to install, calibrate, operate, maintain, and repair the most important biometric systems, i.e., fingerprinting, iris/retina scanning, and voice patterns.
- Understand how the systems interact with other security measures through networked systems.

Extra Desired Knowledge, Skills, and Abilities

- Be familiar with the principles on which other biometric systems, such as facial thermographs, heat generation, and signature dynamics operate and the advantages and disadvantages of each.
- Understand the legal, ethical, and social implications associated with the different biometric systems.

Driving Forces for Employment

Obviously, the most important driving force for employment in the biometrics field is the legislation Congress passed in response to the terrorist attacks on September 11, 2001 (9/11), including legislation that mandates biometrics as prescribed security systems. Relevant legislation is described below:

- The Aviation and Transportation Security Act requires biometric registration for all airport employees. The Act also led to the creation of the Transportation Security Administration’s Registered Traveler Pilot Program, which is exploring the use of biometric keys like fingerprinting and iris scanning as a way to create “trusted traveler” programs that expedite border travel for international travelers. Additionally, the Transportation Workers Identification Card (TWIC) program requires that each of the nation’s 15 million transportation workers, including truck drivers, bus drivers, and airline stewardesses, carry an ID card with some form of biometric identification. The card would contain a photograph, biographical data, and one or more biometric keys.
In June of 2004, DHS awarded a $10 billion dollar contract for the US Visitor and Immigrant Status Indicator Technology (US VISIT) project. The project will provide the capability to record the entry and exit of non-US citizens into and out of the US, and provide officials with biometric information about persons who are in the US in violation of the terms of their admission to the country.

Finally, the Department of Defense (DoD) has established a Biometrics Management Office that will interact with industry, academia, government, and DOD organizations to establish biometric standards and performance measures.

Ratings

State of Maturity Rating: Very Well Structured
Employment Opportunities Rating: Fairly Promising
Current Course Compatibility Rating: Somewhat Compatible
Overall Rating: Somewhat Attractive

State of Maturity

Rating: Very Well Structured

There are a number of technologies embodied in the biometrics area. The most widely used technology is fingerprinting which is a very mature technology. However, even in this area there are a number of new techniques being developed, such as optical, ultrasonic, and chip-based fingerprinting systems, that will require increasing use of new approaches. There are also a number of new technologies that are becoming increasingly popular, such as iris and retina scanning and facial recognition systems. Additionally, a number of techniques are just appearing on the horizon, such as voice recognition, dynamic signature verification, and keystroke dynamics are sparking interest.

It is also important to note that biometric systems interact extensively with secure network technologies that transfer information to and from databases containing enrolled biometric samples and information like terrorist watch-lists and visa information. These network communication, administration, and database systems are based on fairly mature technologies.

The wide range of maturities in this area make it particularly promising for continued viability.

Employment Opportunities

Rating: Fairly Promising

General

Employment opportunities for community and technical college graduates are reasonably good. Realizing the pressing need for individual recognition systems the federal government has reacted quickly including the passage of the Aviation and Transportation Security Act, the Patriot Act, and the Enhanced Border Security and Visa Reform Act, and the initiation of the Transportation Workers Identification Card program. All of these measures have either already become effective or will do so in the near future. Given the number of people and facilities involved, there is every reason to believe that there will be a
need for people that can assist in the installation, calibration, maintenance, repair, and operation of biometric equipment.

A recent market analysis by Frost & Sullivan, reported in the April 2003 edition of Homeland Security Solutions magazine, projects that biometric revenues from commercial applications (not including the government’s AFIS program) will grow from $93.4 million in 2001 to $2.05 billion by 2006. Before 9/11, 2006 revenues were estimated to be in the $700 million range.

Specific employment opportunities for Biometric Systems Specialists and Technicians include:

- Enrollment and transfer of biometric samples into databases.
- Maintenance and repair of commercial facilities’ biometric systems.
- Maintenance and repair of federal government facilities biometric systems.
- Installation and calibration of biometric systems.
- Biometric equipment manufacturing.
- Advising secure installations on biometric systems.
- Inspecting biometric installations to insure that they meet government standards.

Opportunity Timing

The Enhanced Border Security and Visa Reform Act sets a deadline for all border crossings to have “biometric technology” by 2004. Currently, the Transportation Security Agency is soliciting proposals for the Transportation Workers Identification Card and field-testing a wide variety of prototypes.

Special Texas Factors

Obviously, the “biometric registration” requirements set forth in the legislation described in the “Driving Forces” section will have a huge impact on Texas. Airport employees, transportation workers, and people who travel back and forth from Mexico will be required to undergo biometric registration. This will create enormous opportunities in the field. Currently, there are 11 international crossings to Mexico in Texas (Brownsville, Del Rio, Eagle Pass, El Paso, Fabens, Hildago, Laredo, Presidio, Progreso, Rio Grande, and Roma), and the total number of incoming passengers in personal crossings totals about 122,500,000 per year.7

Additionally, Texas has one of the nation’s most extensive air transport systems. There are eight airports – Austin/Bergstrom International, Dallas/Fort Worth International, George Bush Intercontinental in Houston, San Antonio International, Del Rio International, El Paso International, Laredo International, and McAllen Miller International – that offer international service. “Dallas/Fort Worth International Airport, the third busiest passenger airport in the U.S., served more than 55 million passengers in 2001, and George Bush Intercontinental Airport served more than 35 million.”8 Finally, Texas has 29 seaports, thirteen of which are deep water. The Port of Houston handles almost 200 million short tons of imports and exports each year, which makes it first in the United States in foreign waterborne commerce. The demand for biometric solutions at these facilities will be substantial.

7 US Customs Service, Mission Support Services, Office of Field Operations
8 Texas Department of Economic Development www.tded.state.tx.us/business/8.pdf
Current Curriculum Compatibility

Rating: Somewhat Compatible

There are no community or technical colleges in the State with programs that lead to awards in the field of biometrics. However, according to biometric employers, there are programs now being conducted at many colleges that could be expanded to provide students with the KSAs that would qualify them for employment in the identification area. For example, since biometric systems interact extensively with secure information technology networks, biometric employers often seek out people with strong backgrounds in network systems even if they lack biometric experience. It is the belief of these employers that with internal corporate training they can quickly bring such employees “up to speed” on the biometrics portion of the systems they will be servicing.

Several community and technical colleges have programs in network administration and network security that lead to Associates of Applied Science and Certificates of Completion. In addition, many colleges partner with private IT vendors to provide certifications in these areas. Important network administration certifications include the well regarded Certified Cisco Networking Associate (CCNA), the Certified Cisco Internet Engineer (CCIE), the Microsoft Certified Systems Engineer (MCSE), the Certified Novell Netware Engineer (CNE), the Sun Certified Solaris Administrator (SCSA), and the Sun Certified Network Administrator (SCNA). A list of widely regarded network security certifications is provided in the Network Security section of Part I.

Biometric employers also seek out maintenance technicians with strong backgrounds in electronic technology. Since many of these devices are constructed with advanced electronic components, the students they consider hiring typically have completed courses in solid-state circuit design and devices, dc/ac circuits, optoelectronics, microprocessors, and communication circuits.

Employers have indicated that college graduates with network administration/security and/or electronics technology backgrounds with one or two additional survey courses in biometrics would be highly employable. These survey courses would present to students an introduction to the principles of operation, design, testing, and implementation of biometric systems and the legal, social, and ethical concerns associated with their use. In these courses, students would be introduced to a variety of techniques used in the identification and verification of individuals and the physiological basis of these techniques.

Special Instructor Requirements

Instructors must be well trained on each of the major biometric systems currently in use, including most, if not all, of the most widely used commercial products. They must also be knowledgeable of the legal, ethical, and social implication associated with each system. The instructors can become qualified on the various products through training at the manufacturers’ facilities or at places where an applicable system is being applied.

Instructors may wish to take part in one of the two educational programs in Information Assurance and Biometrics developed by the federal Biometrics Management Office (BMO) in partnership with West Virginia University. The first of these programs is a five day Short Course: Concept in Biometrics Systems and Information Assurance, which explores case studies and introduce students to concepts in information assurance, biometrics, testing and evaluation, standards, and socio-legal implications. The second is a 15 credit hour course curriculum that
leads to a graduate certificate in information assurance and biometrics. The curriculum has been designed to teach students about the uses for biometrics, computer network security system principles, the scientific foundation for biometrics, and about social, psychological, ethical and legal policies in the field. The university offers the program through the College of Engineering and Mineral Resources. According to Dr. Walter McCollum, Biometrics Education Program Manager of the BMO, “This program allows participants to combine professional expertise with the course curriculum to gain perspective on public policy, strengthen managerial skills, and interact across agency and executive and legislative branch boundaries.”

Special Equipment Requirements

At a minimum, each community and technical college conducting a course in biometrics systems must have available or access to at least one version of each type of system. Each must also have available necessary tools for testing, repairing, and calibrating each type of system.

It is anticipated that many manufacturers will provide such equipment in order to ensure skilled technicians are available to support their systems. The Texas Technology Initiative may also provide limited funding for equipment purchase. Finally, organizations currently operating biometric systems may allow students to utilize some of their equipment for training purposes.

9 Phone Interview Conducted June 6, 2003
Homeland Security: Network Security

Job Title

Computer Network Security Technician

Job Responsibilities

This person will be part of an information technology group that provides security for an enterprise’s computer networking operations and will ensure that the network is protected from both internal and external threats.

Required Knowledge, Skills, and Abilities

This person will perform vulnerability assessments and install, configure, and maintain a wide variety of networking products (both software and hardware). This person will install and configure internal and external security firewalls and perform network security audits to ensure that there have been no successful breaches of security.

Driving Forces for Employment

The information technology infrastructure of the United States is central to the nation’s economic and public safety infrastructure (i.e. 9/11 system). Due to its central role in these critical activities, public and private enterprises have taken a number of steps to harden this infrastructure against malicious attacks. In fact, President Bush, recognizing the importance of ensuring the continued operation of America’s critical information services, issued the National Strategy to Secure Cyberspace and appointed Amit Yoran, a former vice president at Symantec, as the nation’s cybersecurity chief.

The Strategy states that the “government’s comprehensive strategy to defend cyberspace will be the result of a partnership among government and the owners and operatives of critical infrastructure, including partnerships with the information technology industry, telecommunications, electric power, and the financial services industries.”

Some of the components of this national strategy will include the Department of Homeland requiring federal agencies to increase the efficiency of existing federal cybersecurity programs and promoting private security support for well-coordinated widely recognized professional cybersecurity certifications like the Certified Information Systems Security Professional (CISSP). As a result, Jim Wrightson, VP of Homeland Security at Lockheed Martin, sees an increased demand for network security professionals in the private sector.

Lori Bush, a Senior Adviser in the Cisco Homeland Security group, also projects an increased demand for information assurance and network administrators/security workers in the government sector due to the demands of Homeland Security. “I see a much stronger demand for IT workers at the local, state, and federal level in the next five years. Driving this increased demand, besides specific government initiatives, are three factors: (1) Turnover from the ‘aging’ and subsequent retirement of large parts of the government workforce; (2) Conversion of legacy systems; and (3) The need for skilled network administrators who can provide the necessary security enhancements.”

11 Phone Interview Conducted October 16, 2003
systems to new Internet technology which will require workers skilled in new technologies like gateways; and (3) The need to draw talented IT workers with unique skills from the private sector. In the past many of these workers avoided working for governmental organizations because of pay and prestige concerns.”

Special Texas Factors

The University of Texas at San Antonio, The University of Texas at Dallas, and Texas A&M University have all been designated as National Infrastructure Assurance Centers of Excellence by the National Security Agency.” The program is intended to assist in meeting the national demand for professionals with information assurance expertise in various disciplines. Centers of Academic Excellence in Information Assurance Education are eligible to apply for scholarships and grants through both the federal and Department of Defense Information Assurance Scholarship Programs.”

Ratings

State of Maturity Rating: Very Well Structured
Employment Opportunities Rating: Very Promising
Current Curriculum Compatibility Rating: Very Compatible
Overall Rating: Very Attractive

State of Maturity
Rating: Very Well Structured

A wide variety of technologies, both hardware and software related are utilized in network security. Many of the technologies are widely used (virus protection, firewalls, encryption, intrusion detection), and have been available for some time. Despite their ubiquity, these tools are constantly evolving to meet new threats, therefore, college graduates that enter this field will have to be current on the latest trends. These constantly evolving demands, makes the area particularly promising for continued viability.

Employment Opportunities
Rating: Very Promising

Technical training in network security is needed for employment in a wide range of fields, including software engineering, network administration, banking, e-business, and law enforcement. The occupations that demand these people require a broad spectrum of knowledge and skills, including a significant number that can be filled by people who have completed courses and programs at community colleges. Unfortunately, as Barbara Belton reported in a 2001 NSF funded study, Chief Information Officers believe there is a scarcity of qualified computer security personnel with such training. In fact, her research team found that the vast majority of computer security training programs were at the graduate level (masters and doctorate). The report concluded that “because many positions in the broad

---

12 Phone Interview Conducted October 1, 2003
13 "National Security Agency Centers of Excellence in Information Assurance" http://niatec.info/nsacoe.htm
cybersecurity arena can be filled by workers who hold two-year degrees or who obtain relevant certification, it is natural to assume that there will be a very large number of good, well-paying jobs for students trained in this area.”

Opportunity Timing

Given the current interest in cybersecurity, graduates trained in this area should be able to secure attractive employment immediately upon graduation and demand for qualified personnel will continue to grow for the foreseeable future.

Current Curricula Compatibility

*Rating: Very Compatible*

A number of community and technical colleges award Certificates of Completion or Associate of Applied Science degrees in Network/Computer Security Technology. Students in these programs gain an in-depth understanding of computer networking, operating systems and administration, vulnerability assessments, e-commerce security, encryption, firewalls, anti-virus protection, intrusion detection, and more. Schools looking to establish programs in this area should look to these programs for guidance.

Table 2 Colleges with Awards in Network Security Technology

<table>
<thead>
<tr>
<th>Institution</th>
<th>Award in Network/Computer Security Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dallas Community College District</strong></td>
<td>Certificate in Computer Information Technology – Information Security</td>
</tr>
<tr>
<td>(Cedar Valley, Eastfield, El Centro, Mountain View, North Lake and Richland Campuses)</td>
<td></td>
</tr>
<tr>
<td><strong>Texas State Technical College Waco</strong></td>
<td>Associate of Applied Sciences – Network Security Technology</td>
</tr>
<tr>
<td></td>
<td>Network Security Technology Certificate</td>
</tr>
<tr>
<td><strong>Texas State Technical College Harlingen</strong></td>
<td>Network Security Technology Certificate</td>
</tr>
<tr>
<td><strong>San Antonio Community College District</strong></td>
<td>Certificate in Computer Information Technology – Information Security</td>
</tr>
<tr>
<td>(Palo Alto, Northwest Vista, San Antonio Campuses)</td>
<td></td>
</tr>
</tbody>
</table>

Colleges interested in adding such programs should also seek guidance from the Computer Technology Industry Association (CompTIA) [www.comptia.org](http://www.comptia.org) and the National Workforce Center for Emerging Technologies (NWCET) [www.nwcet.org](http://www.nwcet.org). In June of 2002, NWCET announced a major new agreement with CompTIA and the National Skill Standards Board (NSSB) to develop and promote a uniform set of skill standards for the IT industry. According to a press release announcing the initiative “CompTIA and NWCET – well known for their IT workforce development, education, and certification programs – will also collaborate on joint skill standards, and seek funds from government and private sources for ongoing development of educational and workforce development tools.”

---

14 “Protecting Information: The Role of Community Colleges in CyberSecurity Education,” Report from a Workshop Sponsored by the National Science Foundation and the American Association of Community Colleges 2002
In another component of this initiative, NWCET received an NSF grant to create “CyberSecurity Skill Standards” for graduates at the technician level. Colleges can use the skill standards to create curriculum and courseware development on a national scale.

Additionally, many community and technical colleges throughout the State work with commercial vendors who offer widely respected Certification programs in various Information Technology specialties (e.g. Cisco Academies). By partnering with vendors who offer certification programs related specifically to Network Security, these colleges could offer highly marketable Network Security certification to their students. There are many security certification options, depending on a student’s expertise level and knowledge area. Allan Hoffman, a jobs expert at Monster Tech, in an article entitled “IT Security Certifications” lists and describe some of the most popular and in-demand security credentials. The following descriptions are extracted from that article.

**International Information Systems Security Certification Consortium.** “The nonprofit (ISC)2 offers one of the leading security certifications – the Certified Information Systems Security Professional (CISSP). The CISSP program offers credentials for those responsible for developing and managing the implementation of security policies, standards and procedures. Another (ISC)2 certification, the Systems Security Certified Practitioner (SSCP), is designed for network and systems administrators involved in security implementations.

**Cisco.** “Cisco offers two security certifications. The Cisco Security Specialist certification focuses on demonstrating proficiency in designing, installing and supporting Cisco security solutions. The CCIE Security credential, part of Cisco’s expert-level CCIE (Cisco Certified Internetworking Expert) program, covers security-related topics such as intrusion detection, network design, virtual private networks and firewalls.

**CompTIA Security+.** “CompTIA, the organization behind the A+ and Network+ certifications, has a security credential on topics such as network defense and intrusion detection.

**Symantec.** “Symantec offers two certifications. The Symantec Certified Security Engineer (SCSE) signals in-depth knowledge of a specific area of security expertise such as vulnerability management or intrusion detection. The Symantec Certified Security Practitioner (SCSP) requires expertise across a wide range of security disciplines.

**BrainBench.** “BrainBench offers three security certifications. The Check Point FireWall-1 Administration certification tests Web administrators’ knowledge of Check Point’s FireWall-1 application. The Internet Security credential is designed for network administrators and covers topics such as disaster recovery and encryption. The Network Security credential measures expertise in areas including firewalls, gateways and intrusion detection.

**Check Point.** “Check Point offers three product-focused security certifications. The Check Point Certified Security Administrator (CCSA) is a foundation-level certification for VPN-1/FireWall-1, while the Check Point Certified Security Expert (CCSE) signals higher-level product expertise. Check Point Certified Security Expert Plus (CCSE Plus) focuses on enterprise integration and troubleshooting.

**CIW Security Analyst.** “The CIW Security Analyst certification is designed for networking professionals who want to add a security credential to existing certifications such as the Microsoft Certified Systems Engineer or Certified Novell Engineer.
Global Information Assurance Certification (GIAC). “GIAC offers 10 stand-alone security certifications in specific areas of expertise such as firewalls, intrusion and incident handling. Each may be earned separately, with no particular order required.


TruSecure ICSA Security Practitioner Certifications. “TruSecure plans to offer two security certifications, both backed by its ICSA Labs division. The base-level certification, the TruSecure ICSA Certified Security Associate (TICSA), is designed for system or network administrators with security responsibilities alongside other duties and covers security practices. The TruSecure ICSA Certified Security Expert (TICSE), not yet available, requires more in-depth expertise and design knowledge.”

Special Instructor Requirements

Instructors will have to be familiar with a wide range of technologies related to network security and information assurance: authentication models, protection models, secure programming, intrusion detection and response, operational security issues, physical security, access controls, risk assessment, computer viruses and malware, network firewalls, cryptography, public-key encryption, etc.

In order to meet the demand for trained faculty to develop and teach Information Assurance programs at colleges and universities across the nation, Purdue University is offering an 11 credit hour graduate certificate program for college and university educators who want to develop Information Assurance (IA) programs at their institutions. This project is funded by the National Security Agency Grant Number MDA904-02-1-0203. Funding from the grant will cover tuition, fees, and room and board expenses for selected college and university educators/faculty.

Furthermore, according to its Executive Director, “NWCET is developing a set of cybersecurity modules that will be infused into IT-faculty development programs at its Educator to Educator Institute (E2E), and is designing and developing dynamically publishable cybersecurity courseware which IT instructors may download and use to create personalized textbooks which are timely and relevant for their courses. The goal of this program is to give community college faculty the ability to integrate cybersecurity into their existing and future technician-level IT curricula and the skills and tools necessary to teach those components.”

Job Title

**Chemical – Biological – Nuclear Detection Specialist**

Job Responsibilities

This person will participate in programs designed to detect the presence of weapons of mass destruction.

Required Knowledge, Skills, and Abilities

This person will be familiar with the operation of various sensors used to detect weapons of mass destruction such as ion mobility spectrometry meters (chemical), fourier transform infrared spectrometers (chemical), radiation detection survey meters (nuclear), Geiger counters (nuclear), dosimeters (nuclear), and environmental sensors (biological). The specialist must be capable of interpreting the results such sensors produce.

Driving Forces for Employment

The direct driving force for employment in the chemical-biological-nuclear detection field is the response of federal and state agencies to the terror attacks of September 2001, especially the anthrax mail attacks. For example, departments of public health and safety, once known mostly for regulating the safety of highways, safe drinking water, vaccinations and disease prevention programs, emerged in the wake of these events to play a critical role in the nation’s homeland security plan. According to Retired Major General Todd Stewart, Director of the Program for International and Homeland Security at Ohio State University, “These agencies have made it clear that there is a shortage of skilled lab technicians and equipment qualified to test for the presence of CBN agents.”

To meet this demand, in June 2002, President Bush signed into a law a bioterrorism bill that provided $4.6 billion for improvements to U.S. bioterrorism defenses. Additionally, in June of 2004, the Department of Homeland Security granted $498 million dollars to hospitals nationwide to improve their ability to respond to a biological attack. $33 million dollars of this grant went to hospitals located in Texas. “That money is helping to build better laboratories and better systems for detecting a potential terrorist attack as well as expanded communications systems to get information to public health workers and clinicians quickly,” said CDC Director Julie Gerberding in September 2002. “These investments will not only pay-off in terms of terrorism preparedness, but public health in general will also benefit.”

There is also a critical need for certified professional educational training for first responders in WMD incident awareness, incident command and control systems, and survival planning. 544 Texas jurisdictions recently received $54 million dollars from 2004 First Responder Equipment Grants. The money went to first responders in the State of Texas to fund equipment, training, planning, and exercises that enhance their ability to respond to WMD attacks.

---

18 Phone Interview Conducted June 9, 2003
Ratings

State of Maturity Rating: Fairly Well Structured
Employment Opportunities Rating: Not Very Promising
Current Curriculum Compatibility Rating: Very Compatible
Overall Rating: Not Very Attractive

State of Maturity

Rating: Fairly Well Structured

A number of technologies in various stages of development are being evaluated as a means of accomplishing WMD detection. Some of the detection equipment is quite mature and available commercially – manufactured mostly by Department of Defense (DoD) contractors. Although the technology used in this equipment is fairly mature, many of these currently fielded WMD detection systems also suffer from excessive false positive alarms. This characteristic is highly problematic in civil defense applications, where such alarms could lead to mass hysteria. Therefore, much of the technology in the emerging and forefront stages involves reducing the sensitivity of the equipment to harmless agents, such as pesticides and household cleaners.

Additionally, real-time detection and measurement of biological agents in the environment is extremely difficult because of the “number of potential agents to be distinguished, the complex nature of the agents themselves, and the myriad of similar microorganisms that are a constant presence in our environment and the minute quantities of pathogen that can initiate infection.”20 Only a few civilian agencies, in high probability of attack jurisdictions (e.g. New York, Washington DC) have even a minimal biological agent detection capability. Therefore, first generation technology to accurately measure biological agents is just being developed.

In fact, according to Jack Colley, State Coordinator of the Governor’s Division of Emergency Management - Department of Public Safety, the constantly evolving nature of the threats and technology used in this area, make the knowledge disseminated in CBN detection/awareness programs quite perishable. Therefore, it is essential to continuously update training programs for first responders, a role the State’s colleges already fill quite well for law enforcement organizations.21

Employment Opportunities

Rating: Not Very Promising

Response to a WMD incident will require a multi-discipline/agency response. The disciplines that will be included in the assessment (if present in the jurisdiction) are: law enforcement, emergency medical services, emergency management, fire services, hazardous materials, public works, governmental administrative, public safety communication, healthcare, and public health. Most of these personnel will be first responders and laboratory technicians already employed by government agencies. It is possible, however, that employment opportunities could increase rapidly in the aftermath of a major attack, if the public senses that the response of government agencies was inadequate.

20 Institute of Medicine. Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response National Academies Press 1998
21 Interview Conducted September 12, 2003
Current Curricula Compatibility

Rating: Very Compatible

First responders can never undergo enough training in basic subject matter related to Homeland Security and WMD incident response. According to Jack Colley, some critical skills include: GIS fundamentals (ARCTVIEW), HAZMAT and WMD awareness. Colleges already conduct the bulk of this kind of training for small law enforcement entities. Additionally, the Division of Emergency Management has developed and published a number of guides related to Homeland Security: Texas Facility Security Handbook, Texas Chem-Bio Handbook, Texas School Safety Handbook. Finally, DEM conducted 77,000 hours of Hazard Training statewide in 2002 and has developed a Texas Terrorism Awareness Course for Law Enforcement. The Texas Homeland Security Consortia led by the Lamar Institute of Technology is leading efforts in the State to provide this kind of training.

Departments of Public Health, and possibly the CDC, will continue to hire college graduates with experience and education in clinical chemistry and microbiology principles and techniques. A number of colleges have existing medical technology programs that cover these subjects. Some examples of the kind of microbiology work to be performed include inoculating selective and enrichment media for the purpose of isolating pathogenic microorganisms, preparing final specimens and inoculating definitive media, preparing slides for examination, conducting serological tests, coordinating the proper destruction of discarded tissues and other biologically hazardous material. The Chemical laboratory work to be completed includes preparing standard solutions and reagents for analytical procedures, and assisting in the physical testing and chemical analysis of products, knowledge of the principles and techniques of quantitative and qualitative chemical laboratory tests.

Special Instructor Requirements

Instructors in first responder programs will have to be familiar with a wide range of issues related to chemical, biological, and nuclear weapons. To assist in this endeavor, the Office of Domestic Preparedness provides the nation's first responder training community with a comprehensive training curriculum of over 30 courses in the areas of WMD awareness and crisis planning and management. ODP coordinates this training development and delivery through the Federal Interagency Board and has established a training development and review process. Additionally, ODP has created a network of sites, including one at Texas A&M, where first responders can receive training. For more information on these programs contact the State and Local Domestic Preparedness Expert Assistance Hotline (1-800-368-6498).
Job Title

Chemical – Biological – Nuclear Attack Mitigation Specialist

Job Responsibilities

This person will participate in programs designed to decontaminate people and sites exposed to weapons of mass destruction.

Required Knowledge, Skills, and Abilities

As is the case in industrial hazardous-materials accidents, the first priority in the management of incidents involving weapons of mass destruction (WMD) will be ascertaining the identity and physical properties of the substance that have been released (see Detection Specialist job description). Once the WMD product has been properly identified, the chemical biological nuclear (CBN) Consequences Mitigation Specialist will be responsible for establishing an “effective restricted access outer perimeter, formulating neutralization plans, enacting decontamination procedures and emergency medical treatment plans, and taking environmental preservation precautions.”22

Driving Forces for Employment

A recent Rand Corporation study completed for the CDC, found that there was “widespread confusion among police officers, firefighters, and other emergency workers about the proper response to terror attacks, especially if they involved chemical, biological, or nuclear weapons.”23

In fact to address this problem, 544 Texas jurisdictions recently received $54 million dollars from the Office of Domestic Preparedness to develop and support regional response plans to prepare for possible WMD attacks. The Texas Engineering Extension Service distributed the monies to various county and municipal jurisdictions. The equipment these jurisdictions purchased had to fall within one of 12 categories to qualify for the grant funding. “The categories include personal protective equipment; CBRNE (or chemical, biological, radiological, nuclear, and explosive) search and rescue equipment; interoperable communications equipment; detection equipment; and decontamination equipment. The categories also include CBRNE logistical support equipment; CNRNE incident response vehicles; medical supplies and limited types of pharmaceuticals; and CBRNE reference materials.”24

Ratings

State of Maturity Rating: Not Well Structured
Employment Opportunities Rating: Not Very Promising
Current Curriculum Compatibility Rating: Not Very Compatible
Overall Rating: Not Very Attractive

---

State of Maturity

**Rating: Not Well Structured**

The technologies used to mitigate the effect of attacks with WMDs are very mature. In regards to attacks with nuclear and chemical agents, these technologies include hot-foam scrubbing (radiation mitigation), and high pressure sprayers and detergents (chemical weapons). Mitigating the effects of biological attacks includes vaccines (smallpox) and antibiotics (anthrax). The need for new training programs in these areas is very limited, except as it applies to limited amounts of additional training for first responders. The new technologies that are discussed as a means of mitigating the effect of such attacks are very much in the forefront stage, and do not appear to offer many promising job opportunities in the near future.

Employment Opportunities

**Rating: Fairly Promising**

In normal situations, there is little need for people with special WMD skills. However, if a WMD event occurs, there is an immediate need for many people with these skills. This situation is similar to other disaster events. In Texas, planning for WMD events envisions people and resources being moved from unaffected areas to affected areas. In a serious WMD event, it is probable that federal government, through the National Guard, would also provide people and resources.

Although having WMD Mitigation and Decontamination trained specialists available would be desirable, in reality most training in this area will involve extending the skills of people already involved in public service, e.g., firemen, policemen, nurses, and health care experts. Training of this type will be valuable to people in these professions or planning to enter the profession. However, it appears that the potential for employment of people concentrating in this area will be limited.

Current Curricula Compatibility

**Rating: Very Compatible**

The federal government stands – financially and strategically – at the center of efforts to prepare the Nation’s response to WMD incidents. In a December 2003 article in Government Executive magazine, Paul McHale, the Defense Department’s Assistant Secretary for Homeland Defense, pointed out that ongoing studies have revealed that civilian authorities don’t have the expertise to adequately respond to attacks with WMDs. As a result, the “DoD has brought the National Guard under careful and strategic review and from now on, the Guard will be responsible for robust and critically important homeland defense missions. To supplement those efforts, the Pentagon will increase the number of WMD civil support teams in the National Guard from 32 to 55 in 2004. The teams will work with first responders to detect and react to the use of chemical or biological agents and other weapons of mass destruction. Each team has 22 members and is equipped with mobile laboratories and command posts.”

Most likely, the role of community and technical colleges in this area will involve assisting federal agencies like ODP and the National Guard in the training of first responders in crisis management and control. Any significant curricula, in an area so critical to our Nation’s well being, will probably be federally constructed and directed.

---

Homeland Security: Concealed Explosives

Job Title

Detection Specialist – Concealed Explosives

Job Responsibilities

This specialist will participate in security programs, based around transportation facilities (water ports, airports, cargo ports), designed to detect the presence of concealed explosives.

Required Knowledge, Skills, and Abilities

Explosive Specialists will have to be familiar with the operation of various technologies used to detect such explosives [CT scanners (X-ray), gamma ray (neutron transmission), chemical sniffers, etc.]. There are three possible employment tracks for persons in this field.

Table 3 Explosive Specialist Tasks

<table>
<thead>
<tr>
<th>Subject</th>
<th>Description</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screener</td>
<td>Can provide general, physical, and operational description of explosives detection equipment.</td>
<td>State the purpose of explosive detection equipment and operational characteristics and capabilities; describe all major and associated components including displays, controls and indicators; describe operational tasks.</td>
</tr>
<tr>
<td>Installation Technician</td>
<td>Install explosive detection equipment.</td>
<td>Perform the tasks for installation and operation of explosive detection equipment; adhere to personnel and equipment safety precautions during operations.</td>
</tr>
<tr>
<td>Equipment Maintenance and Inventory Technician</td>
<td>Inventory and maintenance of explosive detection equipment.</td>
<td>Ensure current and complete inventory of all equipment; ensure current maintenance requirements are complete.</td>
</tr>
</tbody>
</table>

Driving Forces for Employment

The immediate driver for employment in this field is the response of federal and state law enforcement agencies to the terrorist attacks of September 2001. However, even before these attacks, the tragic downing of Pan Am Flight 103, the bombing of the Alfred P. Murray Federal Building, and the 1993 attack on the World Trade Center drove home to many Americans the importance of detecting explosives in cargo containers, luggage, and in automobiles before they could be used against critical infrastructure. Listed below are specific regulations and laws related to explosive detection.

Aviation and Transportation Security Act

On November 19, 2001 President Bush signed the Aviation and Transportation Security Act. The Act mandated 100% Explosive Detection Screening (EDS) for checked bags. As a result, over 2000 EDS units were deployed by the end of 2002.
The Maritime Transportation Security Act of 2002

The Maritime Transportation Security Act of 2002 is designed to protect the nation’s ports and waterways from a terrorist attack. The Act requires screening of all “high-risk” cargo and budgeted $90 million dollars in funds for cargo-imaging systems research.

International Ship and Port Facility Code

The 22nd session of the International Maritime Assembly met and unanimously adopted the International Ship and Port Facility (ISPS) Code, which implemented a range of new security measures for ships and port facilities and enhanced existing ones. The measures require compliance by IMO signatory states, and any port or ship doing business with that facility, by July 2004.26

Rex Richardson, Chief Scientist of the SAIC Inspection Operation in San Diego, California, estimates that the Department of Homeland Security (Customs) is currently imaging only 1% of the containers that enter the US. Richardson believes this low inspection rate is not adequate if the country is serious about preventing WMDs and explosives from entering the country. As a result, in the next 8 years, Richardson believes that business for Cargo Inspection could grow from $200 million dollars to $8 billion dollars.27

2004 DHS Budget

The 2004 DHS budget allocated $4.6 billion for the Transportation Security Administration. $400 million dollars has been earmarked for explosives detection systems, including explosive trace detection systems for screening checked baggage. $150 million dollars is for purchasing the explosives detection systems and $250 million will be used to install the equipment in airports.

The Bill also provides $64 million dollars to support technology for non-intrusive inspection (NII). This includes large scale X-ray machines for trucks and oceangoing shipping containers, mobile vehicle and cargo inspection systems (VACIS), and isotope identifiers for international mail and express courier hubs.

Special Texas Factors

Texas supports a state-of-the art transportation and telecommunications network that moves people, products, and information. The criticality of this infrastructure to the State’s well-being, and the need to protect it from attacks, can not be underestimated.

Texas transportation infrastructure includes:28

- 27 airports in 24 cities, 8 of which offer international service
- 29 seaports, including 13 which are deepwater. The Port of Houston leads the US in foreign waterborne commerce
- Forty railroads that employ 12,000 miles of track and ship 300 million tons of freight including chemicals, petroleum, construction materials, transportation equipment and agricultural equipment.

27 Phone Interview Conducted October 15, 2003
Ratings

**State of Maturity Rating:** Very Well Structured

**Employment Opportunities Rating:** Very Promising

**Current Curriculum Compatibility Rating:** Somewhat Compatible

**Overall Rating:** Somewhat Attractive

State of Maturity

**Rating:** Very Well Structured

The X-ray systems and sources used in explosives detection were initially used for medical imaging and then expanded to luggage inspection and non-destructive testing systems in the electronics and other industries. Therefore, these systems are quite mature and have benefited from years of development. However, a number of emerging technologies with the potential of enhancing current capabilities in weapons and explosives detection are being developed. One such technology, called Quadrapole Resonance (QR), uses non-destructive radio waves, that can be easily produced and monitored, to detect explosives. Because it relies on harmless radio waves, QR is considered a very promising detection technique. Additionally, new gamma ray technologies (pulsed fast neutron analysis) make it possible to create 3D scans of a containers interior and determine the chemical composition of objects within the container. It is expected, however that x-ray, gamma ray, and trace detection technology will maintain their dominance in this area until new technologies, like QR, are fully developed and ready for commercial deployment.

Employment Opportunities

**Rating:** Very Promising

Because of the importance of this activity to the well being of the nation, the wide spread recognition of potential threats, the large numbers of exposed facilities, and the federal government regulations described above, this is a field that will see a great expansion over the next few years. Because the threat of terrorist attacks is unlikely to diminish in the foreseeable future it is highly likely that demand for these services will continue for a long time. Moreover, since this area has received little attention in the past, there will be a shortage of well qualified people so that graduates entering the field will have the advantage of attractive employment.

---


Current Curricula Compatibility

*Rating: Very Compatible*

The Texas State Technical College Waco has an x-ray and medical imaging systems program in their biomedical technology department. In fact, according to the 2003 TSTC Waco catalog, it is the first training program in the nation among two-year colleges to provide service technician training for X-ray, computerized tomography, nuclear medicine, and ultrasound equipment. Adding one or two additional classes to such a program that address the specific technical issues related to imaging systems used for explosives detection should be relatively easy. The program, which culminates in an Associate of Applied Science Degree, is outlined in Table 4.

### Table 4  TSTC Waco Medical Imaging Systems Technology Curriculum

<table>
<thead>
<tr>
<th>Class #</th>
<th>Class Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOM 1101</td>
<td>Biomedical Equipment Technology</td>
</tr>
<tr>
<td>BIOM 1209</td>
<td>Applied Biomedical Equipment</td>
</tr>
<tr>
<td>BIOM 1241</td>
<td>Medical Circuits/Troubleshooting</td>
</tr>
<tr>
<td>BIOM 1371</td>
<td>Medical Equipment Networks</td>
</tr>
<tr>
<td>BIOM 1372</td>
<td>Medical Electronics Applications</td>
</tr>
<tr>
<td>BIOM 2201</td>
<td>Safety in Healthcare Facilities</td>
</tr>
<tr>
<td>BIOM 2241</td>
<td>Basic X-ray and Medical Imaging Systems</td>
</tr>
<tr>
<td>BIOM 2335</td>
<td>Physiological Instruments I</td>
</tr>
<tr>
<td>BIOM 2341</td>
<td>General Medical Equipment II</td>
</tr>
<tr>
<td>BIOM 2371</td>
<td>Diagnostic Ultrasound Imaging Systems</td>
</tr>
<tr>
<td>BIOM 2472</td>
<td>R/F X-ray systems</td>
</tr>
<tr>
<td>BIOM 2473</td>
<td>Digital Radiography</td>
</tr>
<tr>
<td>BIOM 2474</td>
<td>Advanced Imaging Systems</td>
</tr>
<tr>
<td>BIOM 2680</td>
<td>Cooperative Education – Biomed Engineering Related Technology</td>
</tr>
</tbody>
</table>
Job Title

*Critical Infrastructure Security Specialist*

Job Responsibilities

This person will work within organizations that design and execute complete security plans for critical infrastructure. These specialists will focus on the protection of people and tangible assets.

Required Knowledge, Skills, and Abilities

The tasks of Critical Infrastructure Security Specialists will include vulnerability assessment and mitigation (i.e. building inspections), security regulation documentation, and security program management. Abilities will include a familiarity with the various technologies used to secure access to critical assets (metal detectors, access cards, surveillance cameras, exterior perimeter breech warning systems, etc.). These specialists will also perform other activities to ensure compliance with national standards related to security (building and fire codes).

Driving Forces for Employment

The *National Strategy for Physical Protection of Critical Infrastructures and Key Assets*, which was constructed in the wake of the 9/11 attacks, provides a list of recommendations that “state and local governments, private sector entities, and concerned citizens across America can take to enhance our collective infrastructure and asset security.”

The strategic objectives that form the foundation of the Nation’s infrastructure and key asset protection effort include:

- Identifying and assuring the protection of those infrastructure and assets the Nation deems most critical.
- Providing timely warning and assuring the protection of those infrastructures and assets that face a specific, imminent threat.
- Assuring the protection of other infrastructures and assets that may become targets over time by pursuing specific initiatives and enabling a collaborative environment between the public and private sector.

The policies and procedures that government and private sector entities adopt to meet these objectives will be a driving force for employment.

---

Ratings

State of Maturity Rating: Very Well Structured
Employment Opportunities Rating: Very Promising
Current Curriculum Compatibility Rating: Very Compatible
Overall Rating: Very Attractive

State of Maturity
Rating: Very Well Structured

A number of technologies, some mature and others emerging and forefront, are being explored to aid the nation in its quest to protect critical infrastructure. The mature technologies include smart access cards with biometric keys, walk-thru weapon detectors, surveillance cameras, and alarm systems. Some emerging technologies include long-range infrared imaging systems (night-vision), vehicle-stopping systems (nets that can catch cars going 60 miles per hour), unmanned aerial vehicles (drones) with night vision/detection capabilities, etc. Technologies at the forefront include surveillance cameras with algorithms that are capable of automatically detecting “suspicious behavior” and speech patterns in airports and other public areas. This mix of technologies, and the willingness of organizations to pay for their implementation, will play a large part in shaping job opportunities in this area.

Employment Opportunities
Rating: Very Promising

There is an enormous amount of critical infrastructure that must be protected from terrorist attacks (see Table 5), and there will be tremendous job opportunities in this area involving installation, calibration, maintenance, testing, and repairing equipment; in designing protection systems; and in supervisory activities.

For example, the Port of Corpus Christi is implementing $1.8 million dollars in security upgrades. “The money will go towards the purchase of various high-tech security systems and devices, including advanced technology that automates threat detection through real-time analysis.”32 Adesta LLC, which is installing the security upgrades for the port, will provide cameras, intrusion detection technology, fencing, sensors, and an access control system, on a fiber-based communications network that transmits data to a central control room.

Table 5 The Protection Challenge

<table>
<thead>
<tr>
<th>Resource</th>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture and Food</td>
<td>1,912,000 farms</td>
</tr>
<tr>
<td></td>
<td>87,000 food processing plants</td>
</tr>
<tr>
<td>Water</td>
<td>1,800 federal reservoirs</td>
</tr>
<tr>
<td></td>
<td>1,600 municipal waste water facilities</td>
</tr>
<tr>
<td>Public Health</td>
<td>5,800 registered hospitals</td>
</tr>
<tr>
<td>Emergency Services</td>
<td>87,000 U.S. localities</td>
</tr>
<tr>
<td>Defense Industrial Base</td>
<td>250,000 firms in 215 distinct industries</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>2 billion miles of cable</td>
</tr>
<tr>
<td>Energy</td>
<td></td>
</tr>
<tr>
<td>Electricity</td>
<td>2,800 power plants</td>
</tr>
<tr>
<td>Oil and Natural Gas</td>
<td>300,000 producing sites</td>
</tr>
<tr>
<td>Transportation</td>
<td></td>
</tr>
<tr>
<td>Aviation</td>
<td>5,000 public airports</td>
</tr>
<tr>
<td>Passenger Rail and Railroads</td>
<td>120,000 miles of major railroads</td>
</tr>
<tr>
<td>Highways, Trucking, and Busing</td>
<td>590,000 highway bridges</td>
</tr>
<tr>
<td>Pipelines</td>
<td>2 million miles of pipelines</td>
</tr>
<tr>
<td>Maritime</td>
<td>300 inland/costal ports</td>
</tr>
<tr>
<td>Mass Transit</td>
<td>500 major urban public transit operations</td>
</tr>
<tr>
<td>Banking and Finance</td>
<td>26,600 FDIC insured institutions</td>
</tr>
<tr>
<td>Chemical Industry and Hazardous Materials</td>
<td>66,000 chemical plants</td>
</tr>
<tr>
<td>Postal and Shipping</td>
<td>137 million delivery sites</td>
</tr>
<tr>
<td>Key Assets</td>
<td></td>
</tr>
<tr>
<td>National Monuments and Icons</td>
<td>5,800 historic buildings</td>
</tr>
<tr>
<td>Nuclear Power Plants</td>
<td>104 commercial nuclear power plants</td>
</tr>
<tr>
<td>Dams</td>
<td>80,000 dams</td>
</tr>
<tr>
<td>Government Facilities</td>
<td>3,000 government owned/operated facilities</td>
</tr>
<tr>
<td>Commercial Assets</td>
<td>460 skyscrapers</td>
</tr>
</tbody>
</table>

*These are approximate figures.

Source: National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

Current Curricula Compatibility

**Rating: Very Compatible**

Critical Infrastructure protection encompasses a broad range of disciplines taught in the State’s community and technical colleges. Table 6 lists some of those disciplines and how they have or might impact critical infrastructure (CI) initiatives, broken down by task:
### Table 6 Critical Infrastructure Tasks

#### Prevention of Attacks Against Critical Infrastructure

<table>
<thead>
<tr>
<th>College Program</th>
<th>Technology Utilized</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aviation Maintenance</td>
<td>Unmanned Aerial Vehicles</td>
<td>UAVs to patrol airspace above CI.</td>
</tr>
<tr>
<td>Electronics Technology</td>
<td>Sensors, Actuators (magnetic locks), Video Surveillance</td>
<td>These technologies will be used in intrusion alert and access control systems.</td>
</tr>
<tr>
<td>Electromechanical Systems</td>
<td>Equipment, Radar, Proximity Detectors</td>
<td></td>
</tr>
<tr>
<td>Control Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer and Network Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X-ray Imaging Systems</td>
<td>Explosives and Weapon Detection Equipment</td>
<td>Prevent these kind of attacks on and within CI.</td>
</tr>
</tbody>
</table>

#### Mitigation of Consequences of an Attack Against Critical Infrastructure

<table>
<thead>
<tr>
<th>College Program</th>
<th>Role</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building and Construction</td>
<td>Building Codes</td>
<td>New codes may mandate improved building materials, enabling stronger, longer-lasting CI able to withstand attacks, be they bridges, buildings, or off-shore oil rigs.</td>
</tr>
<tr>
<td>Technology</td>
<td>Fire Codes</td>
<td></td>
</tr>
<tr>
<td>Architectural Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fire Protection Technology</td>
<td>Firefighting Tactics/ Strategies</td>
<td>New information may be helpful to firefighters in predicting the likely behavior of future large-scale fires in high-rise buildings.</td>
</tr>
</tbody>
</table>

#### Response to an Attack Against Critical Infrastructure

<table>
<thead>
<tr>
<th>College Program</th>
<th>Role</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications Technology</td>
<td>Wireless Voice Transmission</td>
<td>New wireless voice inter operability equipment and standards can enhance communications between diverse organizations with different radios and frequencies during an incident.</td>
</tr>
<tr>
<td>Geographic Information Systems</td>
<td>Emergency Management GIS</td>
<td>Provide info to first responders that allows them to establish evacuation routes, and restricted access perimeters.</td>
</tr>
</tbody>
</table>
**Job Title**

*Pattern Analyst*
*Data Miner*
*Database/Data Warehouse Administrator*

**Job Responsibilities**

Database/Data Warehouse Administrators will be responsible for the design and management of the database/data warehouse systems used in organizations that collect information vital to Homeland Security. This person will work with distributed, heterogeneous, and multimedia databases.

Pattern Analysts and Data Miners will use analytical software tools to detect “suspicious” patterns in multiple sets of data. As such, this person will identify behaviors that are considered outliers or deviations from “the norm” (for example, excessive purchase of chemicals that could be used to create bombs or chemical weapons) and overlay that information with data from government databases and data warehouses (arrest records, suspected terrorist lists, INS data, etc.). The purpose of such analysis is to identify, track, and prevent hostile actors from attacking the Nation.

**Required Knowledge, Skills, and Abilities**

Database/data warehouse administrators will have to be competent in current database technology, which goes beyond traditional relational databases to “encompass technologies for storing and searching multimedia data (e.g., images, audio, speech, graphics, animation, video), free-form text files, and semi-structured data such as HTML and XML.”\(^{33}\) These technologies are, and will continue to be, key elements of the intelligence tools such as data mining and link analysis, used to enhance Homeland Security.

Pattern analysts will have to be competent in their understanding of analytical techniques and their value in generating strategic knowledge. These persons will possess a wide range of knowledge and skills including assessing data integrity, statistical methods, data mining and a familiarity with the privacy and civil liberty concerns such work generates. They will (1) apply their data mining skills using sophisticated software tools, (2) develop logic and reasoning as aids to complex problem solving, and (3) gain exposure to statistical concepts and their application.

**Driving Forces for Employment**

Obviously, the driving force for employment in this field is the response of federal and state law enforcement agencies to the terrorist attacks of September 2001. As President Bush pointed-out “in an address to the nation after the attacks, information on the hijackers’ and their activities was available through a variety of databases at the federal, state, and local government levels as well as within the private sector.”\(^{34}\) If this information had been combined and analyzed in an appropriate manner, law enforcement agents might have been able to “connect the dots” and prevent the attacks. In fact, Oracle Homeland Security Solutions views the problem of homeland

---


\(^{34}\) White House. “Using 21st Century Technology to Defend the Homeland” *Securing the Homeland Strengthening the Nation* 2001
security as essentially an information management problem – in other words how can the
government take information from disparate information communities (INS, FBI, CIA, local and
state law enforcement), analyze it, and quickly transmit intelligence to people who can act on it
and prevent terrorist acts.35

As a result, the Defense Department’s DARPA (Defense Advanced Research Projects Agency)
has launched the Terrorist (formerly Total) Information Awareness (TIA) Initiative to help
protect the US from future terrorist attacks. The purpose of the initiative is to “integrate public
and private databases of all data relevant to monitoring the activities of potential terrorists and
their supporters, and querying, analyzing, and mining the data.”36 Furthermore, President Bush
has authorized the creation of the Terrorist Threat Integration Center in part to allow integrated
access to various databases of the US federal government, including the Department of
Homeland Security, the CIA, and the FBI, etc. Integrated access to these databases should allow
these agencies to share information effectively and identify and track suspected terrorists and
their supporters in a more timely fashion. In essence, with each of these initiatives, the federal
government is creating central data warehouses, out of what was once separate and disparate
databases. The information in this warehouse can be queried and analyzed to produce timely,
accurate actionable intelligence about terrorists and their activities.

However, before these tools can be placed into operation, a number of issues related to privacy
and civil liberties must be addressed. With the FBI’s powers greatly expanded under the Patriot
Act, some fear that the innovations being put into place are just the first steps in establishing a
“Big Brother” police state.

Ratings

State of Maturity Rating: Well Structured
Employment Opportunities Rating: Promising
Current Curriculum Compatibility Rating: Quite Compatible
Overall Rating: Quite Attractive

State of Maturity

Rating: Well Structured

Although the software, statistical, and database technologies used in this area are widely
used, like most information technology items they are constantly evolving and becoming
more powerful. Examples of this evolution include: (1) new technologies that simplify the
integration of data from databases with distinct architectures and schema (i.e. hetero-
genous databases); (2) real-time data warehouses that allow intelligence analysts to
instantaneously detect and respond to suspicious patterns in massive datasets; and finally
(3) multimedia databases that allow users to query by multimedia content (shape, color,
speech, etc).

Additionally, on the data mining side of the equation, pattern analysts will have to be
competent in their understanding of emerging analytical techniques and their value in
generating strategic knowledge related to Homeland Security. Finally, these workers will
have to be familiar with the privacy and civil liberty implications of their work and its

35 Phone Interview with Steve Cooperman, Vice President, Oracle Homeland Security Solutions conducted October 1, 2003
relation to ever changing public opinion and laws. Therefore, this range of technology maturities and the requirement of competencies in a wide range of fields (software, statistics, law) makes the area particularly promising for continued viability.

**Employment Opportunities**

**Rating: Fairly Promising**

Employment opportunities in this area should be considered in two parts:

**Database and Data Warehouse Administrators**

Steve Cooperman, Vice President of Oracle Homeland Security Solutions, a division of the largest information management company in the world, believes that people with information technology and management skills (databases, data warehouses), who have a solid understanding of the mission of the organizations they support, will be highly employable. The technical skills these people will need include (1) enterprise database skills and (2) programming skills in languages, like XML and JAVA, that form the backbone of application integration servers.37

**Pattern Analysts**

Although interest in the use of pattern analysis techniques has been growing over the last few years, at present it appears that positions for two-year college graduates will be limited in the near future. Moreover, there are a number of privacy issues to be resolved before law enforcement use of analysis/mining becomes pervasive. A number of United States Senators, including Dianne Feinstein (D-CA), and some influential members of the news media (William Safire, New York Times) are calling for a moratorium on the use of data mining technology in the TIA initiative in particular and on US homeland security in general until the issues of civil liberties and privacy are fully debated and addressed.

**Current Curricula Compatibility**

**Rating: Quite Compatible**

Many Texas community and technical colleges have Database Administration programs. The curricula in these programs, which are typically centered around database platforms developed by Oracle and Microsoft, the two largest database vendors, include courses in client/server programming, programming languages such as Visual C++, Visual Basic and PL/SQL (Standard Query Language) as well as web-based implementation of database technology. In some of the more advanced programs, students install and administer their own database management systems, and study the advanced concepts of distributed databases and data warehousing. Adding additional classes to these programs that address the specific technical issues related to data mining (e.g. multimedia search) should be relatively easy.

Additionally, many colleges partner with private I.T. vendors to conduct programs that give students certification in specific database platforms. Some important database certifications include:

**Oracle.** “Oracle Certified Professionals- Database Administrators have proven skills managing a large-scale database or developing applications that are deployed enterprisewide. The OCP-DA credential covers topics such as database architecture and administration, database backup and recovery, and performance tuning.”38

---

37 Phone interview conducted October 1, 2003
38 "Oracle8i Certified Professional Database Administrator." www.oracle.com/education/certification/index.html?dba8i_ocp.html
Microsoft. “Microsoft Certified Database Administrators (MCDBA) must demonstrate they have the skills necessary to successfully design, implement, and administer Microsoft SQL Server™2000 databases. Candidates need to pass three core exams and one elective exam that provide a valid and reliable measure of technical proficiency and expertise in the implementation and administration of SQL Server databases.”39

IBM. “IBM Certified Database Administrators (MCDBA) must demonstrate they have the skills necessary to successfully design, implement, and administer IBM DB2 V8.1 databases. Candidates have to demonstrate a knowledge of SQL and DB2 authentication and authorization.”40

Teradata. “Teradata Certified Administrators (TCA) have proven their ability to implement, tune, and maintain a Teradata database for a production environment. Candidates have a thorough understanding of capacity planning, workload optimization, security, backup/recovery, and release management.”41

There are no community or technical programs in data mining in the state.

40 “DB2 Information Management.” www-306.ibm.com/software/data/education/cert/
Federal Programs

Since the events of September 11, 2001 a number of groups have initiated various HS training and educational projects. Although most of these projects involve training for first responders, there are also projects focusing on other HS areas. The key federal government agency charged with developing and enhancing the capacity of state and local governments to prepare for and respond to threats or acts of terrorism involving weapons of mass destruction is the U.S. Office of Domestic Preparedness (ODP). ODP has developed a Three-Year Statewide Domestic Preparedness Strategies paper that provides guidance for state HS agencies. In addition to providing guidance on technical assistance, equipment grants, and exercises, the paper provides guidance for training programs. Specifically, the training program:

- Provides the nation’s first responder community with a comprehensive training curriculum of over 30 courses in the areas of awareness, performance, and management and training.
- Coordinates training development and delivery through the Federal Interagency Board.
- Establishes training development and review process.
- Utilizes distance-learning tools to maximize impact.

Training areas to be addressed include:

- Determining training needs.
- Identifying training resources.
- Evaluating locally developed WMD courses.

Private and College Programs

In addition to the federal and state government programs, a number of private organizations and colleges have initiated HS training programs. A review of these programs provided below can be useful to colleges considering initiation of HS programs.

The AACC Ad Hoc Task Force on Homeland Security

“On January 21, 2004, in response to a growing need to develop better training and new programs related to HS, the American Association of Community Colleges (AACC) announced the appointment of a 21-member task force to define a long-range strategy for the nation’s 1,173 two-year colleges. The AACC Ad Hoc Task Force on Homeland Security comprises 18 community college presidents including Margaret Forde (Houston Community College System) and Herlinda Glasscock (Dallas County Community College District) and three senior specialists at institutions with advanced programs and demonstrated expertise in defense and security. Members were chosen based on well-established relationships they have with four-year colleges and universities, as well as with state and local security providers. The AACC Task Force held a Feb. 8 meeting in Washington, D.C., to coalesce and coordinate homeland security efforts already well underway at community colleges around the nation. Task Force members will serve for approximately two years.”

League for Innovation in the Community College

The League for Innovation in the Community College is an international consortium serving community colleges. In February of 2003, “the League hosted a Homeland Security Summit to (1) begin a dialogue about existing Homeland Security and prevention programs being offered by community colleges and (2) to identify unmet needs. Thirty-seven leaders from League member colleges and partners gathered in Tempe, Arizona to help frame a national community college readiness and prevention initiative. Presentations were made by institutions with existing Homeland Security programs, including public safety and law enforcement, first responder training, health care, biotechnology, cyber security, hazardous materials, mass fatalities, disaster recovery, international relations, language training, and community awareness and engagement.”44

In February of 2004, the League and the Community College National Center for Community Engagement hosted a second Homeland Security and Civic Engagement Summit to “help community colleges create and improve homeland security training and education programs that emphasize community engagement. The 2004 Summit offered research and theories, strategies, and tips and techniques for connecting homeland security academic curriculum to civic engagement. Participants from all disciplines attended.”45

National Academic Consortium for Homeland Security

“The National Academic Consortium for Homeland Security (NACHS) comprises public and private academic institutions engaged in scientific research, technology development and transition, education and training, and service programs concerned with current and future U.S. national security challenges, issues, problems and solutions, at home and around the world. Currently, 85 colleges and universities are members of the coalition.

“The goal of the National Academic Consortium for Homeland Security is to help improve the security of the U.S. and its worldwide interests, while protecting and preserving its values, freedoms and civil liberties, and economic interests and competitiveness. The specific objectives of the Consortium are to help:

- Improve understanding of national security issues, especially terrorism and strategies for counter-terrorism.
- Promote development of better-informed public policy, strategy, plans and programs regarding national security issues.
- Develop new technologies and transition those technologies into effective, practical and affordable solutions to (current and future) international and homeland security problems.
- Educate and train the people required by governmental and non-governmental organizations, to effectively accomplish international and homeland security roles and responsibilities.

“The primary role of the consortium is to promote, support and enhance academic research, technology development, education and training, and service programs dealing with all aspects of international and homeland security, through collaboration and information-sharing among academic institutions, researchers and scholars. The NACHS vision is that

45 “Homeland Security and the Community College: A Vibrant Present and Vital Future”
the consortium will become an effective sounding board and consultative body to assist federal-government decision makers in developing more effective national policies and programs concerning academic research and technology development, education and training, and related service programs pertaining to national security.”

A listing of HS programs provided at member institutions can be found at https://newman.uts.ohio-state.edu/nachs/siteSearch.cfm.

**American Institute of Homeland Defense**

“One of the most interesting organizations in the HS area is American Institute of Homeland Defense (AIHD) www.americanihd.com located in San Antonio, Texas. AIHD works in partnership with WMH Associates, SpecTal, LLC, and Arrow Mountain. WMH, working in the role of subcontractor, assists American Military University (AMU) in the design, development, and instruction of counter-terrorism educational courses. SpecTal provides specialized consulting services to the U.S. Government and to the private sector. Arrow Mountain offers comprehensive emergency management planning encompassing the full spectrum of business continuity planning.

“AIHD is also associated with Lamar Institute of Technology (LIT) in Beaumont, Texas, St. Phillips College in San Antonio, Texas, Houston Community College, Texas State Technical College in Harlingen, Texas, Southwest Texas Junior College in Uvalde, Texas, Brooklyn College in Brooklyn, New York. LIT has been designated as a Homeland Security National Center of Excellence, while Brooklyn College and St. Phillips College have been designated Regional Centers of Excellence. Penn State University and several other colleges are reportedly negotiating with AIHD to join the program.

“AIHD courses are delivered in 8-hour blocks, and carry professional education credit for law enforcement, private security and other personnel. Each course is 8 weeks in length followed by an 8 hour end-of-course seminar, completed either on-site or by viewing the end-of-course seminar via CD/DVD. Courses currently being offered are:

- IS100 - Introduction to Terrorism
- IS101 - Domestic Terrorism
- IS102 - The International Terrorist
- IS103 - Mind of a Terrorist
- IS200 - Terrorist Tactic
- IS201 - Intermediate Terrorism
- IS202 - Islamic Fundamentalism

The courses are worth three semester hours of college credit, and can be applied to Associates and Bachelors degree programs offered through American Military University. Students who complete five of the seven courses earn a Certificate in Counter Terrorism Fundamentals.”

**Center for Infrastructure Assurance and Security**

“The University of Texas at San Antonio has established The Center for Infrastructure Assurance and Security (CIAS) to leverage San Antonio’s Infrastructure Assurance and Security (IAS) strengths as part of the solution to the nation’s Homeland Defense needs and deficit of IAS talent and resources. The CIAS has successfully integrated academic,

---

46 www.osu.edu/homelandsecurity/NACHS/index.html
government, and industry efforts resulting in a dynamic organization dedicated to infrastructure assurance, research and education. CIAS envisions developing an education pipeline of IAS talent to increase the number of students who will study infrastructure assurance and security, ultimately earning degrees that will contribute to the IAS field in San Antonio and the nation.\(^4^8\) The Center will concentrate its effort in the following areas.

- Intrusion Detection
- Wireless Encryption
- Steganography
- Dark Screen
- Biometrics
- Forensics
- Infrastructure Vulnerabilities
- Computer Crime (with FBI)
- Data Mining
- Database

**Homeland Security Training Alliance**

Another organization involved in HS education is the Homeland Security Training Alliance (HSTA). The purpose of the HSTA is to provide uniform Terrorism Preparedness oriented training programs for community and technical colleges in Ohio.

“Training will be provided to firefighters, law enforcement, hospitals, public health departments, public works employees, business and industry, and school safety and security personnel – all critical first responders in every community, who not only respond to terrorist attacks, but accidents, and natural disasters as well. The HSTA was formed to fill the gaps in the statewide training efforts, not to take the place of existing and successful training programs already underway.

“The HSTA has selected The University of Findlay (UF)’s Center for Terrorism Preparedness (located in Findlay, Ohio) as the first course provider for this effort. One of UF’s well-established courses has been selected for the initial pilot. Soon, other course providers, such as the State Fire Academy will be selected as well, in order to accommodate the requests from certain communities, and to assure that quality and timely programs are offered statewide. Courses being planned include:

- **For First Responders:**
  - WMD Awareness
  - WMD Operations
  - WMD Technician

- **Incident Command**
  - Public Health/Medical Courses
  - Hospital Emergency Incident Command System (HEICS)
  - Basic Anti-Terrorism Emergency Life Saving Skills (4 & 8 Hr)
  - Bioterrorism and Emerging Disease Recognition and Overview (4 & 8 Hr)

\(^4^8\) [http://cias.utsa.edu/](http://cias.utsa.edu/)
• Law Enforcement Courses
  • Intelligence Collection
  • Securing our Critical Assets
  • Anti-terrorism Planning

• Additional Courses
  • Public Utilities – Risk Assessment Methodology for Water Utilities
  • Corporate Safety & Security – Workplace Violence and Terrorism Update
  • School Security – Preventing Targeted Violence in Schools

“The HSTA has initiated both a Curriculum Development Committee and a Trainer Qualifications Committee to assure the courses meet existing training standards, and that the trainers possess the qualifications necessary to deliver the courses. These committees have members from several campus locations as well as first responder communities. The association is incorporating more first responder community members, as well as working on additional key partnership opportunities.”

Center for Education and Research in Information Assurance and Security

“To enhance the public’s understanding and acceptance of information protection through awareness, training, and education, Purdue University has recently established the Center for Education and Research in Information Assurance and Security (CERIAS).

“CERIAS offers courses, products, articles, and resources geared towards a variety of audiences, including business and industry, home users, educational institutions, and the government. The vision of CERIAS is to establish an ongoing center of excellence which will promote and enable world class leadership in multidisciplinary approaches to information assurance and security research and education. This collaboration will advance the state and practice of information security and assurance. The synergy from key members of academia, government, and industry will promote and support programs of research, education, and community service.

“CERIAS emphasizes its multidisciplinary approach to the problems, ranging from purely technical issues (e.g., intrusion detection, network security, etc) to ethical, legal, educational, communicational, linguistic, and economic issues, and the subtle interactions and dependencies among them. The research conducted through CERIAS includes faculty from six different schools and 12 departments across campus. The eight areas below summarize the research focus areas for the faculty involved with the center.

• Risk Management, Policies, and Laws
• Trusted Social and Human Interactions
• Security Awareness, Education, and Training
• Assurable Software, and Architectures
• Enclave and Network Security
• Incident Detection, Response, and Investigation
• Identification, Authentication, and Privacy
• Cryptology and Rights Management

“In Summer 2003, CERIAS conducted an eight-week, eleven credit-hour program for faculty members from colleges in several states in the area of Cyber Security. The courses included in this program can be found in Appendix E. CERIAS plans to conduct a similar program in Summer 2004 for a broader audience.”  

Other Programs

In addition to these coordinated programs a number of colleges and universities, including community and technical colleges have initiated courses in HS. Among others these include:

**Lamar Institute of Technology**

LIT has received national recognition as being among the first colleges to offer HS training. LIT is a member of the National Academic Consortium of Homeland Security and has been designated a Homeland Security National Center of Excellence, by the American Institute of Homeland Defense.

LIT is a member of the Homeland Security Curriculum Development Consortium that includes Houston Community College, Dallas Community College, Texarkana College, Texas State Technical College Harlingen, Texas State Technical College Waco, El Paso Community College, St. Phillips, South Texas Community College (McAllen), Amarillo College, Del Marr College, Southwest Texas Junior College (Uvalde), Midland College, and Kilgore College. The college will participate in a National Homeland Security DACUM September 17-19, 2004 at the Houston Bush International Airport Marriott.

**West Virginia University**

West Virginia University, in coordination with the U.S. Department of Defense Biometrics Management Office, has developed a Graduate Certificate Program in Information Assurance and Biometrics that will be offered through the College of Engineering and Mineral Resources. The program includes courses in biometric systems and information assurance, as well as computer security and advanced study of biometric and forensic statistics, digital image processing, and computer network security (see http://www.lcsee.cemr.wvu.edu/biometrics/certificate.php). The University is also conducting a five-day short course in “Concept in Biometric Systems and Information Insurance” (see Appendix F for course outline).

**Monroe Community College**

Monroe Community College (MCC) in Rochester, New York has launched a Homeland Security Management Institute. The stated goal of the Institute is to prepare “business and industry, public officials, schools, citizens and first-responders for public safety crises.” The Institute will be a regional source for homeland security training of first-responders, elected officials, citizens and professionals whose jobs may place them in a leadership or response role in a homeland security emergency.” Although the Institute is based in

---

50 [www.cerias.purdue.edu](http://www.cerias.purdue.edu)
51 [www.lcsee.cemr.wvu.edu/biometrics/5daycourse.php](http://www.lcsee.cemr.wvu.edu/biometrics/5daycourse.php)
New York, its’ leadership envisions a role for the Institute in the national homeland security training picture. For example, MCC plans to create training programs that other community and technical colleges can license and use within their own programs.

Cincinnati State Technical and Community College

Cincinnati State Technical and Community College has expanded its EMT training to address issues related to Homeland Security. For example, “the college is currently designing an advanced HAZMAT course that provides introduction into military grade chemical weapons and basic detection capabilities for Weapons of Mass Destruction (WMD) training.”53 Additionally, the college has constructed a new training center, classrooms, lab, and drill area that trainers and students can use for chemical and radiation safety topics.

Texas A&M University

“Through its National Emergency Response and Rescue Training Center, Texas A&M University delivers a set of courses to prepare public officials, emergency medical services, law enforcement, fire protection, and public works for the threat posed by weapons of mass destruction. Courses are developed and designed to provide each specific segment of the emergency response community with the tools needed to accomplish its role in the event of a WMD incident. Additionally, Texas A&M has developed an Interactive Internet WMD Awareness Course for emergency responders. Texas A&M also provides technical assistance to state and local jurisdictions in the development of WMD assessment plans through the Texas Engineering Extension Service (TEEX). TEEX offers the following courses of instruction: WMD Threat and Risk Assessment, WMD Incident Management/Unified Command, Emergency Response to Terrorism Basic Concepts, Emergency Medical Operations, and WMD Awareness (Internet course). For additional information on TEEX courses contact TEEX at www.teexwmdcampus.com or nerrtc@teexmail.tamu.edu.”54

As discussed in Part One of this report, review of relevant literature and discussions with various experts in the Homeland Security (HS) field indicated that there were seven categories of HS specialists in which the graduates of the Texas community and technical colleges might find attractive employment. These categories are:

- Identification
- Network Security
- Weapons of Mass Destruction (WMD) Detection
- WMD Mitigation and Decontamination
- Concealed Explosives
- Critical Infrastructure Security
- Pattern Analysis/Data Warehouse Administration

In Part One, information, concepts, and suggestions were made to assist community and technical college instructional officers in evaluating, initiating, and conducting HS programs in their individual colleges. In this part of the report, the technological underpinnings for each of these categories will be presented.
The terrorist attacks of September 11, 2001 brought immediate attention to the challenges of authenticating the identity of individuals living in or attempting to enter the United States. Identifying persons with hostile intent and preventing their access to sensitive materials, assets, or public infrastructure became a high priority. The realization of these challenges resulted in an intensified effort to develop identity authentication tools that could not be duplicated, lost, or loaned.

**General**

Authentication processes fall into three general categories:

- Authentication of a person for entry into a system or area.
- Authentication of individual input material, e.g., messages, into a system.
- Authentication of the person seeking to extract information from a system.

Approaches to authentication are based on:

- What you have, e.g., electronic pass keys, smart cards, or tokens.
- What you know, e.g., passwords or PIN numbers.
- Who you are, e.g., physical characteristics and identifiable action patterns.

Techniques based on “who you are” are generally referred to as “biometric” technologies.

Biometric technology involves the automatic identification or identity verification of an individual based on measurable physiological and/or behavioral characteristics. With the introduction of biometrics there is a shift in focus from a knowledge-based recognition system, i.e. what you have and what you know, towards the presence of a physical or behavioral trait, i.e., who you are. Biometrics are the only keys that cannot be lost, stolen, or given away, and therefore represent the highest level of security. Thus, by direction, this forecast will focus on that approach. However, one interesting example of the “what you know” approach will be discussed in the section describing facial recognition techniques.

Typically, biometric authentication involves three tasks:

- Enrollment: Capturing a sample of one or more unique personal characteristics (physiological or behavioral) and then processing the sample to produce a reference for the individual concerned.
- Association: Compression, processing, and comparison with one or more stored samples.
- Verification: Interfacing with one or more IT systems to verify information and/or confirm the identity of the enrollee.

Often, authenticated identification of the sender will imply authentication of the input material. In many cases, the techniques utilized to authenticate the person introducing information into the system or withdrawing material for the system are similar to the techniques utilized to gain access to restricted facilities. Commercial biometric systems for specialized applications like these have existed for more than 20 years.

The use of various techniques for authentication purposes can be done in one of two ways: to make a “one-from-one” match, or a “one-from-many” match. That is to say, the system can compare an input sample with an identified stored sample, or find a match for the input sample from a large number of possible samples.
Biometric Technologies

The technologies required in biometric authentication fall into two categories, those involved in capturing the characteristic sample (principally hardware) and those involved in matching candidate samples with stored samples (principally software).

There are a number of personal characteristics currently being used or considered for biometric authentication. Those based on physiological characteristics include:

- Fingertips
- Eye Characteristics (retina and iris)
- Facial Characteristics
- Hand Geometry (one finger, two finger, and whole hand)
- Ear Characteristics
- Overall Body Heat Pattern

Those based on behavioral characteristics include:

- Voice Recognition
- Dynamic Signature Verification
- Keystroke Dynamics
- Gesture Analysis

Determining which biometric is appropriate for a specific application requires a thorough understanding of the different strengths and weaknesses of each approach. It must be stated that no one approach is perfect, and few, if any, systems are as good in the real world as they are under controlled conditions in the lab. For example, missing limbs render hand geometry and fingerprinting biometrics applications useless. "Cataracts can pose problems for iris and retina biometrics, while manual laborers may have worn away their fingerprints. Eyeglasses and long hair can interfere with the operation of facial recognition systems, and unlike people, biometrics do not age, making re-enrollment necessary."\(^{55}\)

However, all of the news on this front is not negative. Voice recognition biometrics are ideal for telephone transactions and handwriting biometrics work well for document security and financial or insurance applications. "Voice and signature have the added benefit that the enrollment is easy: a subject simply speaks or signs. A face, fingerprint, iris, hand, or other biometric, while very accurate, can take a skilled attendant to explain the enrollment process to newcomers and even then, automated enrollment is not guaranteed."\(^{56}\)

A description of the operating characteristics and the advantages/disadvantages of various biometric systems is discussed below.

Physiological Characteristics

Fingerprints

For large-scale positive identification applications, no currently available biometric technique is comparable with fingerprinting. Traditional fingerprint identification techniques are well established, proven, legally accepted, and mature.

---


\(^{56}\) Hardin, Winn. "Biometrics Measure up Homeland Security."
Techniques for recording, archiving, and matching fingerprints have been generally available for many years. The basic principle of fingerprint identification is that the fingers of each person have a pattern of “whorls,” “arches,” “loops,” “hooks,” and other shapes unique to that individual. For identification, a single print or a set of prints of a known individual is compared to that (those) of the person to be authenticated. The steps typically involved in fingerprint identification are:

- Collect constant fingerprint characteristics, i.e., those that remain valid for a lifetime such as overall shape, number of lines, distances between specific points.
- Classify fingerprints, i.e., utilize main fingerprint shapes to identify them with a group of individuals
- Identify with certainty, i.e., utilize fine structure (minutaes) of prints to identify specific individual.

Traditionally, fingerprints have been recorded using ink images on paper. For the purposes authenticating large numbers of people who must be identified at any number of locations, this approach has obvious shortcomings.

**Figure 1 iGuard3 FPS 110 Fingerprint Access Control System**

More recent techniques include:

- **Optic systems.** In this technique, the finger is placed on a platen, usually made of glass, and a picture of the finger is taken. This is the oldest and most mature technology, except for the ink-on-paper technique.

- **Ultrasonic system.** In this technique, the finger is placed on a platen and an ultrasonic image recorded. Since sound is used for the recording, intimate contact with the platen is not necessary, and usable prints can be recorded even if thin latex gloves are used or if the fingers are dirty. Although this technique has been available for a number of years, acceptance has been limited.
• **Chip-based systems.** In this technique, the finger is placed directly onto a specially designed silicon chip and the image recorded electronically. For example, in the Capacitive system, sensors register the fingerprint by interacting with the electric field variations produced by the skin’s ridges and valleys. The chip then creates an electrical image of the fingerprint. The compact one-chip system is smaller in size than optical systems and requires ultra-low power, consuming less than 1 milliWatt at 5 Volts. It also generates a higher quality image than most other identification methods. According to Erik Bowman of Identix Corporation, “the largest application of fingerprint technology is in automated fingerprint identification systems (AFIS) used by police forces throughout the U.S. and in over 30 foreign countries. These multi-million dollar installations have been responsible for thousands of criminal apprehensions and increasingly are being used for non-law enforcement applications, such as welfare benefits and border crossings, military facilities including the Pentagon, and government labs. Machines, however, tend to reject over 3% of authorized users while maintaining false accept rates of less than one in a million.”

**Eye Characteristics (Retina and Iris)**

**Technologies & Techniques Used:**

- **Retina recognition.** This technique utilizes a template of the layer of the blood vessels located at the back of the eye (retina). These patterns of retina are scanned by a low intensity light source via an optical coupler and analyzed for characteristic points within the pattern. Retinal systems look similar to an eye test where put the subject places his/her eye to a viewer while an invisible infrared light illuminates the back of the eye and a camera takes a picture of the vein pattern.

![Figure 2 EYEDENTIFYÔ Retina Reader with Keypad](image)

*Courtesy: Access Controls International*

- **Iris imaging and recognition systems.** This technique uses a video camera to capture a sample of the pattern of the iris (the colored portion of the eye). The sample may include corona, crypts, filaments, freckles, pits, radial furrows, and striations. Software is used to compare resulting data against stored templates. The technique is less intrusive than retina recognition, requires no intimate contact between user and recorder, and is

---

generally considered to be highly accurate. This technique is considered to be a great source of identification because the iris is stable throughout one’s life, it is not susceptible to wear and injury, and it contains a pattern that is unique to an individual. This technique is further advanced and more widely utilized than retina recognition.

**Facial Characteristics**

This technique is based on the use of certain facial characteristics that are unique to an individual. With the increase in the number of video cameras, the use of face recognition as an identification system becomes more attractive to both the consumer and the business. The public appears to accept the use of this technique at levels similar to public acceptance of the use of static photographs.

**Technologies & Techniques Used:**

- **Eigenface.** In this method a human face is represented as a linear deviation from a mean or average face. It is presumed that every face can be assigned a “degree of fit” to each of the 150 eigenfaces. The eigenface information is derived from a computer-based analysis of the digital image of a photo. Eigenhead is a 3D version of Eigenface that also analyses the shape of the head.  
  
- **Facial metrics.** Two approaches are used in the application of this technique. The first compares feature sizes and relationships, such as nose length and the distance between the eyes. The second matches the most significant image data, like the size of your nose, with a record of the face stored in a database.

- **Face monitoring.** This technique utilizes face recognition technology to monitor the attendance of an authenticated end-user at a desktop.

- **Facial thermograms.** This technique senses heat patterns in the face caused by the flow of blood under the skin for authentication.

- **Passface.** Although this technique utilizes a “what you know” approach rather than the “who you are” approach, it is based on similar theoretical underpinnings as the face recognition techniques discussed above. Based on the ability of the human mind to remember faces, the user memorizes four faces and then logs onto a system by identifying these faces from a random arrangement of decoy faces. Passface has used this ability to remember and recognize faces as the basis of a “cognometric” identity verification system. The system was developed and patented by ID-Arts (Visage Developments, Ltd), a UK company, in September 1997. At the end of 1997, Paul Barrett took over management of ID Arts, which he restructured and relocated to the USA as Real User Corporation. As an alternative to biometrics, “cognometrics” requires no special hardware and is inexpensive and user friendly. The Passface™System is supported by extensive academic research and by experiments conducted by Professor Hadyn Ellis, Head of the School of Psychology at University of Wales Cardiff. The research behind this system goes back to the 1970s when efforts on machine recognition of faces began.

---


59 “Real User.” [www.realuser.com/cgi-bin/ru.exe/_/homepages/index.htm](http://www.realuser.com/cgi-bin/ru.exe/_/homepages/index.htm)

Hand Geometry (one finger/two finger, palm and whole hand)
The finger/hand geometry techniques are easy to use and tend to appeal to public because it does not raise many privacy issues. Systems based on these techniques are generally fast and have low data-storage requirements. However, they are less accurate than some other approaches.

Hand geometry techniques are over 20 years old. In that time, six different hand-scanning products have appeared on the market, “including the most commercially successful biometric to date, the Handkey from Recognition Systems, Inc. The Handkey looks at both the top and side views of the hand using a built-in video camera and compression algorithms. Dirt and cuts do not detract from performance, and the hand can be guided easily into the correct position for scanning.”61 Hand geometry has been deployed at thousands of locations including hospitals, day care centers, welfare agencies, the Colombian legislature, San Francisco International Airport, and immigration facilities for the INS Passenger Accelerated Service System (INSPASS) frequent international traveler system. The technique was also used for security at the 1996 Olympic Games in Atlanta.62
Devices that examine other features of the hand are being developed. These include:

- **Finger Geometry.** One or two fingers are placed beneath a camera that captures the shapes and lengths of the areas of the finger and the knuckles. To determine identity, the system captures a three-dimensional image and matches the data against the stored templates.

- **Palm recognition.** The palm is placed on a hand reader and the reader captures the three-dimensional image of the various textures (ridges and other minutiae) of the palm.

- **Hand geometry.** The hand is placed on a hand reader and the reader captures the three-dimensional image of the fingers and knuckles and stores the data in a template.

**Ear Characteristics**

At present there does not appear to be any organization actually using ear shape as a basis of authentication. However, the use of the ear shape to identify a person is being studied by the University of Linz in Austria and Dr. Mark Burge of Armstrong Atlantic State University (University of Georgia System).63

**Overall Body Heat Patterns**

Although the use of overall body heat patterns has been suggested as a possible authentication technique, there does not appear to be any organization offering a system for commercial use nor is anyone actually using the technique for authentication.

**Behavioral Characteristics**

**Voice Verification**

This technique identifies individuals by comparing their voice/speech patterns with patterns already on file. In using the technique, the system creates a template based upon numerous characteristics, including cadence, pitch, tone and shape of larynx. Although the voice pattern is determined to large extent by the shape of the throat and larynx, this biometric technique is considered to be a hybrid of physiological and behavioral because there is the possibility that a user can alter his/her speech to generate a false rejection. Background noise is also an issue that could affect the template.

**Technologies & Techniques Used:**

- **Text-dependent system** (aka fixed-text system). This system requires a speaker say a specific set of numbers or words.

- **Text-independent system** (aka free-text system). This system creates voiceprints from unconstrained speech and does not require a speaker to say a specific set of numbers or words.

- **Speaker separation.** This system separates overlapping voices from each other and other background noises.

- **Voiceprint.** This system utilizes a representation of the acoustic information found in the voice of a speaker. Time series of spectral-power-density plots, which show how the energy in your voice at different frequencies varies versus time as you vocalize a word or phrase.

---

63 www.computing.armstrong.edu/FacNStaff/burge/research/biometrics.html
**Dynamic Signature Verification**

This system measures the distinguishing features of both the signature and the process of signing. It analyzes the way an end user signs his/her name. It examines such things as speed, stroke order, stroke count and pressure exerted by a hand holding a pen, as well as the end product of the signature. Though this biometric technique tends to be more acceptable to the public than most other systems, the verification is considered to be one of the least accurate biometrics. This is due to the fact that the technology measures a behavioral characteristic and users can easily change their signature to generate a false rejection. “Despite this fact, over 100 patents have been issued in this field, including several each to IBM, NCR and VISA. Several other companies currently have commercial products available.”

Communication Intelligence Corporation [www.cic.com](http://www.cic.com) is the leading supplier of biometric electronic signature verification solutions including paperless workflow, handheld computers, and smartphones.

**Technologies & Techniques Used:**
- **Acoustic emission.** This proprietary technique records the movement of a pen tip over a paper fiber to generate acoustic emissions that are transmitted in the form of stress waves within the material of a writing block beneath the document being signed. Structure-borne elastic waves behave in materials in a similar way as sound waves in air and can be detected by a sensor attached to the writing block.

**Keystroke Dynamics**

This technique, currently under development, analyzes typing rhythm when an end-user types certain characters onto a keyboard, such as their user name and password.

**Gesture Analysis**

Although the use of gesture analysis has been suggested as a possible authentication technique, there does not appear to be any organization offering a system for commercial use.

---

Dynamic Growth

The commercial biometric industry is aggressive, dynamic, and growing. The biometrics industry is generally divided into two segments, automatic fingerprint identification systems (AFIS) and the remaining market. “While the government AFIS market is quite mature, served by a few biometrics companies working in concert with prime contractors to the government, such as TRW, Unisys, Siemens, Raytheon, and Lockheed Martin among others, major growth in AFIS is expected to come from expanding commercial markets that have crossed over with government agencies.” According to biometric analyst Prianka Chopra of market analysis firm Frost & Sullivan in San Jose, California, “biometric revenues from commercial applications (not including the government’s AFIS program) will grow from $93.4 million in 2001 to $2.05 billion by 2006. Before 9/11, 2006 revenues were estimated to be in the $700 million range. Additionally, Chopra estimates that the AFIS market “will grow from $246 million in 2001 to $453 million by 2006, a jump of 13 percent.” The US VISIT and Transportation Worker Identification Card (TWIC) programs will contribute to this growth. There is a large amount of volatility in the biometric identification industry. Several mergers, acquisitions, or new alliances, new product announcements, new joint projects, and new major contracts, are signaling maturation of the industry. Commercially available biometric authentication systems include the following:

Fingerprints

More than 50 companies currently offer products in the finger scanning and processing area. Among these products are:

- **Ultrasonic finger systems.** UltraScan (licenses technology to Kodak and others).
- **Chip-based systems.** FingerChip3 by Thomson-CSF, Fingerprint ID by Siemens, SmartFinger by STMicroelectronics, FPS 200 by Veridicom, and Fingerloc by Authentec.
- **Forensic AFIS (Automatic Fingerprint Identification Systems) software.** Motorola (Printrak International) (leading fingerprint recognition systems provider), SAGEM MORPHO, SUN, NEC, Cogent, TRW, and Titan.
- **Civil AFIS applications hardware.** SAGEM MORPHO, Dermalog, Digital Biometrics, Cross Check, Indentix, TRW, and Neurodynamics.

Other fingerprinting companies include Astro Datensysteme AG, Atmel, Bergdata Biometrics GmbH, BEC, BES, Biolink, BMF, Cansec, Cherry, Security First (Ethentica), Exact ID, Fingerprint Cards AB, Fujitsu, Indivos, Keico Hightech, Key Source, Keytronic, LabCal, Precise Biometrics, Print Electronics, SecuGen, TST, Ultra-Scan, and VeriFone.

---

Eye Characteristics

- **Iris imaging systems.** Iridian Technologies of Moorestown, NJ and Geneva, Switzerland, is the sole owner and developer of US and international patents on the core authentication technologies based on iris recognition. The company licenses the technology to several other companies including Diebold.

- **Retina scanning.** Only one company, EyeDentify, Inc., with one product, EyeDentify Biometric Retina Reader, has ever offered a retinal scan device, and no others are expected to enter the field. The Reader is sold by both EyeDentify and a handful of physical security distributors, including Access Controls Incorporated.

Facial Characteristics

- **Face recognition.** Identix, Human Scan GmbH, AcSys Biometrics, Cognitec, and Viisage. Viisage's TrueFace ID™ product compares individual faces obtained from a live or taped video feed with a database of subjects to identify pre-selected security risks. The technology captures the face of a person, recognizes who that person is, and stores that person's image for future analysis.

Hand Geometry

- **Hand recognition.** Recognition Systems (leading hand geometry recognition biometric vendor), BioMet Partners (two-finger geometric profiling), and Apogee Biometrics (palm scanner).

Voice Verification

- **Voice Recognition.** Scansoft (Speechworks), Graphco Tech, Sentry Com, VeriVoice, Voice Security, Qvoice, and Nuance Communications.

- **Voice verification algorithm.** Noise Cancellation Technologies, Inc. (NCT) licenses ClearSpeech™.
**Dynamic Signature Verification**

- **Signature Dynamics.** MmiGroup, Wondernet Communication Intelligence Corporation, Cyber SIGN Inc., and ePad™ developed by Interlink Electronics, captures handwritten signatures for use in PC applications.

**Keystroke Dynamics**

- **BioPassword.** The BioPassword software system creates an individual profile based on a user’s typing rhythm. The software measures this typing rhythm against a stored biometric template that includes information about a user’s typing speed and keystroke characteristics. The company offers the system in conjunction with fingerprinting technology to provide a two-layered approach to network security.
As indicated above, the market for biometric authentication systems is growing rapidly and a number of companies, particularly small ones, are investigating new approaches for accomplishing the authentication purpose. One of the results of these research and development efforts is the realization that there are a number of physiological and behavioral characteristics that are essentially unique to individuals. In addition to the more commonly used characteristics such as fingerprints and voice recognition, more esoteric patterns such as body heat generation, odors, physical gestures, and ear shapes are being more or less actively examined. Therefore, it is useful to review industry trends, as well as technology trends, and to examine some emerging technologies of interest.

**Industry Trends**

Ever increasing pressure to reduce cost, size, and scanning and processing times. One of the main roadblocks to acceptance of biometric systems has been their relatively high cost. These costs are now decreasing dramatically. For example, the smallest fingerprint reader sold by Identix Incorporated, the BioTouch PC Card, costs about $150. In 1994, the smallest fingerprint reader sold by the company was the size of a telephone and cost $2,000.

**Increased industry standardization**

It appears that the issue of compatibility among different software and hardware systems has been emerging as this industry has begun to expand its products and services into the private sector. For example, the Executive Board of the International Committee for Information Technology Standards “established Technical Committee M1, Biometrics, in November 2001 to ensure a high priority, focused, and comprehensive approach in the United States for the rapid development and approval of formal national and international generic biometric standards. The M1 program of work includes biometric standards for data interchange formats, common file formats, application program interfaces, profiles, and performance testing and reporting. The goal of M1’s work is to accelerate the deployment of significantly better, standards-based security solutions for purposes, such as, homeland defense and the prevention of identity theft as well as other government and commercial applications based on biometric personal authentication.”

**Recognition of the need for public acceptance**

For biometric technology to gain wide acceptance in the consumer and business markets, several issues will need to be taken into consideration. The first is public acceptance of the replacement of PINs and other recognition techniques with biometric technology. With the issue of identity verification, comes the issue of an individual’s privacy. The industry will need to develop products that improve security without encumbering users and that provide a high level of convenience to customers. Recognizing these challenges, leading biometric manufacturers formed the International Biometric Industry Association in September of 1998 to advance, advocate, defend and support the collective international interests of the biometric industry.

---

68 “M1-Biometrics.” www.ncits.org/tc_home/m1.htm
Other factors that must be considered are the legal issues involved with introducing biometrics into society. Laws requiring a signature or photograph on certain documents will have to allow for the substitution of biometric identity-verification techniques. Also, laws concerning privacy will be an area that must be considered as biometric technology becomes more widespread. In fact on May 27, 2003, with many members citing concerns about privacy, the Texas House of Representatives voted 111 to 26, to kill a bill (S.B. 945) that would have authorized the Department of Public Safety to automate the scanning of biometric images of Texans’ faces and fingerprints.

**Technology Trends**

In addition to the general industry trends noted above, there a number of technology trends to be noted.

**Increasing use of multiple authentication techniques**

To accomplish ever-higher levels of security, many companies are now developing systems that apply several authentication approaches simultaneously, e.g., spoken passwords combined with speech identification. The integration of several physiological and/or behavioral characteristics to provide multiple means of identity verification can enhance authentication reliability. Such integration takes advantage of the capabilities of each biometric characteristic and overcomes some of the limitations of a single biometric process. When tested independently, identity established by such an integrated system has proven to be more reliable than identity established by individual biometrics. These multiple characteristic processes also provide for increased security. To meet targeted reliability thresholds, it is anticipated that the industry will look towards products that will incorporate multiple biometrics. Examples of multi-biometric efforts within the industry include BioID, a multi-biometric product developed by HumanScan, which uses face, voice, and lip movement recognition to uniquely identify a person. The system is low cost (only requires a standard USB camera and microphone) and is easy to use and unobtrusive (users simply look into a camera and say, for example, their name).

**Integrated Technologies – Infrastructure Concerns**

Biometric systems impact the physical and information technology infrastructure of organizations. The effect of a biometric system on everything from telephone lines to existing security systems and IT networks must be considered when installing a system because biometrics impacts them all. “The potential complexity of a biometric security system has created an integrator industry that brings together many disciplines. Companies like Curtiss-Wright in Lyndhurst, N.J. and Advanced Biometric Security (ABS) in Littleton, M.A. have made a business out of combining biometrics to meet individual applications. In addition to understanding the population, conditions, biometrics, and infrastructure involved with a system, companies like ABS bring server and database expertise critical to efficiently interfacing with existing IT networks without adversely impacting the network.”

---

Furthermore, because biometric systems can impact so many other systems critical to an institution, the biometric industry is attracting larger players in addition to start-ups. For example, the US VISIT program calls for the installation of biometric technology at all US crossings by the end of 2004. The installation of such systems will have a huge impact on a wide variety of areas: the physical infrastructure of border crossing and security checkpoints, government communication and information technology architectures, the ease at which millions of people can move across the border, etc. Accenture, the prime contractor leading the project, has comprehensive expertise in managing large-scale, mission critical system integration projects for the U.S. government. Accenture will work closely with experienced biometric software and hardware providers to create cost effective and efficient Secure Border systems that meet the varied needs of the nation.

Because of the dynamic nature of the biometric authentication industry, the Homeland Security Community has, and will have available to it, a wide variety of biometrics products and services. Moreover, the ever changing nature of the industry and the very aggressive research and development activities that characterize it, will require colleges interested in conducting programs in this field to keep up to date on the technological state of the art.
General

Weapons of mass destruction fall into three general categories:

**Chemical.** Mustard gas and simple chemical agents such as phosgene, hydrogen cyanide. Also more complex weapons such as nerve agents GA (tabun), GB (sarin), GD (soman), and VX.

**Biological.** Living microorganisms and viruses (anthrax, ebola, smallpox). Also toxins, which are nonliving chemicals manufactured by bacteria, fungi plants, and animals. The two toxins most important to this discussion are botulinum toxin (of which botulinum toxin A is the most toxic for humans) and staphylococcus enterotoxin B (SEB), an incapacitating toxin.

**Nuclear.** Radiation delivered by traditional nuclear military weapons and also dirty bombs.

Chemical Detection Technologies

**Chemical Weapons**

A wide variety of chemical detection equipment for first responders is available commercially and through the Department of Defense. This equipment can be either mobile or stationary and can be used to detect chemical agents at a single location (point source) or remotely (stand-off). Table 7 lists various detection equipment technologies and their capabilities. A comparison of the sensitivity column in Table 7 and the data in Table 8 reveals that most of the detection devices are capable of detecting immediately dangerous concentrations of chemical agents.\(^\text{71}\)

\(^{71}\) Institute of Medicine. *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response* National Academies Press 1999.
### Table 7 Chemical Detectors

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Agent</th>
<th>Sensitivity</th>
<th>Time</th>
<th>Cost</th>
<th>Operations/ Maintenance/ Limits &amp; Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>M-8 Paper</strong></td>
<td>Nerve-G</td>
<td>100-µ drops</td>
<td>&lt;=30 sec</td>
<td>$1 per book of 25 sheets</td>
<td>Disposable/hand held; Dry, undamaged paper has indefinite shelf life. Chemical agent detector paper; 25 sheets/book and 50 booklets/box; potential for false positives.</td>
</tr>
<tr>
<td></td>
<td>Nerve-VX</td>
<td>100-µ drop</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mustard-H</td>
<td>100-µ drops</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Liquids only</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>M-9 Paper</strong></td>
<td>Nerve-G</td>
<td>100-µ drops</td>
<td>&lt;=20 sec</td>
<td>$5 per 10-m roll</td>
<td>Disposable/hand-held 3-year shelf life Carcinogen. Adhesive-backed dispenser roll or books.</td>
</tr>
<tr>
<td></td>
<td>Nerve-VX</td>
<td>100-µ drops</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mustard-H</td>
<td>100-µ drops</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Liquids only</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>M-18A2</strong></td>
<td>Nerve-G</td>
<td>0.1 mg/m³</td>
<td>2–3 min</td>
<td>$360</td>
<td>Disposable tubes Hand-held. 25 tests per kit; Detector tubes, detector tickets, and M-8.</td>
</tr>
<tr>
<td><strong>Detector Kit</strong></td>
<td>Nerve-VX</td>
<td>0.1 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mustard-H, HN, HD, HT</td>
<td>0.5 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lewisite-L, ED, MD</td>
<td>10.0 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phosgene-CG</td>
<td>12.0 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blood-AC</td>
<td>8.0 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Liquid, vapor, aerosol</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>M-256A1</strong></td>
<td>Nerve-G and VX</td>
<td>0.005 mg/m³</td>
<td>15 min</td>
<td>$140</td>
<td>Disposable Hand-held 5-year shelf life. Each kit contains 12 disposable plastic sampler-detectors and M-8 paper.</td>
</tr>
<tr>
<td><strong>Detector Kit</strong></td>
<td>Mustard-HD</td>
<td>2.0 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lewisite</td>
<td>9.0 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phosgene oxime-CX</td>
<td>3.0 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blood-AC, CK</td>
<td>8.0 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Vapor or liquid</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>M-272 Water Test Kit</strong></td>
<td>Nerve-G and VX</td>
<td>0.02 mg/l</td>
<td>7 min</td>
<td>$189</td>
<td>Portable/lightweight 5-year shelf life USN, USMC. Used to test raw or treated water; Type I and II detector tubes, eel enzyme detector tickets; Kit conducts 25 tests for each agent.</td>
</tr>
<tr>
<td></td>
<td>Mustard-HD</td>
<td>2.0 mg/l</td>
<td>7 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lewisite</td>
<td>2.0 mg/l</td>
<td>7 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hydrogen cyanide</td>
<td>20.0 mg/l</td>
<td>6 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CAM Chemical Agent Monitor</strong></td>
<td>Nerve-GA, GB, VX</td>
<td>0.03 mg/m³</td>
<td>30 sec</td>
<td>$7,500</td>
<td>Hand-held/portable battery operate–8 hours continuous use. Maintenance required. Radioactive source. False alarms to perfume, exhaust paint, additives to diesel fuel.</td>
</tr>
<tr>
<td></td>
<td>Blister-HD and HN</td>
<td>0.1 mg/m³</td>
<td>&lt;=1 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Vapor only</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ICAM Improved Chemical Agent Detector</strong></td>
<td>Nerve-G and V</td>
<td>0.03 mg/m³</td>
<td>10 sec</td>
<td>$7,500</td>
<td>4.5 pounds Minimal training. Alarm only; False positives common.</td>
</tr>
<tr>
<td></td>
<td>Mustard-HD</td>
<td>0.1 mg/m³</td>
<td>10 sec</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ICAM-APD Improved Chemical Agent Detector–Advanced Point Detector</strong></td>
<td>Nerve-G</td>
<td>0.1 mg/m³</td>
<td>30 sec</td>
<td>$15,000</td>
<td>12 pounds including batteries Low maintenance Minimal training. Audible and visual alarm.</td>
</tr>
<tr>
<td></td>
<td>Nerve-V</td>
<td>0.04 mg/m³</td>
<td>30 sec</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mustard-H</td>
<td>2.0 mg/m³</td>
<td>10 sec</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lewisite-L</td>
<td>2.0 mg/m³</td>
<td>10 sec</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ICAD Miniature Chemical Agent Detector</strong></td>
<td>Nerve-G</td>
<td>0.2–0.5 mg/m³</td>
<td>2 min</td>
<td>$2,800</td>
<td>8 oz pocket-mounted 4 months service No maintenance Minimal training. Audible and visual alarm; Marines; No radioactivity.</td>
</tr>
<tr>
<td></td>
<td>Mustard-HD</td>
<td>10 mg/m³</td>
<td>(30 sec for high levels)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lewisite-C</td>
<td>10 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cyanide-AC, CK</td>
<td>50 mg/m³</td>
<td>2 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phosgene-CG</td>
<td>25 mg/m³</td>
<td>15 sec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chemical Agent Detector</td>
<td>Chemical Agent</td>
<td>Sensitivity</td>
<td>Response Time</td>
<td>Price</td>
<td>Remarks</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>-------------</td>
<td>---------------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>M-90 D1A</td>
<td>Nerve-G, V</td>
<td>0.02 mg/m³</td>
<td>10 sec</td>
<td>$16,000</td>
<td>15 lb. with battery. Radioactive source exempt from licensing. Minimal training only. Ion mobility spectroscopy and metal conductivity technology can monitor up to 30 chemicals in parallel. Alarm only.</td>
</tr>
<tr>
<td></td>
<td>Mustard</td>
<td>0.2 mg/m³</td>
<td>10 sec</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lewisite</td>
<td>0.8 mg/m³</td>
<td>80 sec</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blood</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MM-1 Mobile Mass</td>
<td>Nerve-GA, GB, GD</td>
<td>0.2 mg/m³</td>
<td>&lt;=2 min</td>
<td>$2,555</td>
<td>Vehicle battery operated. Maintenance required. Radioactive source (license required); Automatic unattended operation; Remote placement.</td>
</tr>
<tr>
<td>Spectrometry</td>
<td>Nerve-VX</td>
<td>0.4 mg/m³</td>
<td>&lt;=2 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gas Chromatograph</td>
<td>Mustard-HD</td>
<td>10 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MM-1 Mobile Mass</td>
<td>Nerve-G</td>
<td>90 mg/m³</td>
<td></td>
<td>$110,000</td>
<td>Line-of-sight dependent. 10 year shelf life. 2-person portable tripod. Passive infrared energy detector 3 miles; Visual/audible warning from 400 meters.</td>
</tr>
<tr>
<td>Spectrometry</td>
<td>Mustard-H</td>
<td>2,300 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lewisite-L</td>
<td>500 mg/m³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MM-1 Mobile Mass</td>
<td>Nerve-GB</td>
<td>1.0 mg/m³</td>
<td>1 min</td>
<td>$5,500</td>
<td>Minimal training. Field use. Alarm only; False alarms from gasoline vapor, glass cleaner.</td>
</tr>
<tr>
<td>Spectrometry</td>
<td>Nerve-GD</td>
<td>0.12 mg/m³</td>
<td>1 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mustard-HD</td>
<td>0.6 mg/m³</td>
<td>1 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vapor</td>
<td>&lt;=45 sec</td>
<td></td>
<td>$300,000</td>
<td>Military $100,000 civilian</td>
</tr>
<tr>
<td>MM-1 Mobile Mass</td>
<td>Nerve-G</td>
<td>&lt;0.0001 mg/m³</td>
<td>&lt;5 min</td>
<td>$34,000</td>
<td>Designed for field industry monitoring (10 lb.) 8 hours training 24 hour/7 day operations. Plug-in modules increase versatility; Threshold lower than AEL.</td>
</tr>
<tr>
<td>Spectrometry</td>
<td>Mustard-H</td>
<td>&lt;0.003 mg/m³</td>
<td>&lt;5 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lewisite-L</td>
<td>&lt;0.003 mg/m³</td>
<td>&lt;5 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MM-1 Mobile Mass</td>
<td>Nerve-G, V</td>
<td>&lt;0.001 mg/m³</td>
<td>&lt;10 min</td>
<td>$100,000</td>
<td>Field use, but 85 pounds needs 120v AC, helium 40 hours training. Lab quality analysis; Library of 62,000 chemical signatures.</td>
</tr>
<tr>
<td>Spectrometry</td>
<td>Mustard-HD</td>
<td>&lt;0.003 mg/m³</td>
<td>&lt;10 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GC/MS</td>
<td>Many others</td>
<td>&lt;0.001 mg/m³</td>
<td>&lt;10 min</td>
<td>$50,000</td>
<td>Not designed for field use. Gas, air, 220v AC 40 hours training. State-of-the-art gas chromatograph; Used by CWC treaty lab.</td>
</tr>
<tr>
<td>HP 6890 GC with Flame</td>
<td>Nerve-G, V</td>
<td>&lt;0.001 mg/m³</td>
<td>&lt;10 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photometric Detector</td>
<td>Mustard-HD</td>
<td>&lt;0.0006 mg/m³</td>
<td>&lt;10 min</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response Institute of Medicine, National Academies Press
Table 8 Estimated Human Exposure Guidance for Selected Chemical Warfare Agents

<table>
<thead>
<tr>
<th>Agent</th>
<th>Vapor (mg/m³)</th>
<th>EC₅₀</th>
<th>Liquid ED₅₀ (mg/70 kg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tabun (GA)</td>
<td>0.0001</td>
<td>&lt; 1.7</td>
<td>&lt; 880</td>
</tr>
<tr>
<td>Sarin (GB)</td>
<td>0.0001</td>
<td>&lt; 0.8</td>
<td>1,000</td>
</tr>
<tr>
<td>Soman (GD)</td>
<td>0.00003</td>
<td>&lt; 0.8</td>
<td>200</td>
</tr>
<tr>
<td>VX</td>
<td>0.00001</td>
<td>&lt; 0.3</td>
<td>&lt; 2.5</td>
</tr>
<tr>
<td>Sulfur mustard (HD)</td>
<td>0.003</td>
<td>3.33</td>
<td>600</td>
</tr>
</tbody>
</table>

Source: (AEL) Edgewood Safety Office, 1996; (ED₅₀) National Research Council; (EC₅₀)

**AEL:** The maximum airborne exposure concentration for an 8-hr workday.

**EC₅₀:** The airborne concentration sufficient to induce severe effects in 50% of those exposed for 30 minutes.

**ED₅₀:** The amount of liquid agent on the skin sufficient to produce severe effects in 50% of the exposed population.

The M8 and M9 papers provide inexpensive, rapid results (<1 minute) concerning the presence of liquid mustard and nerve agents. The papers are just screening tests, however, and their results must be substantiated with much more accurate detection tests. This is particularly true when one considers the fact that the papers often generate positive results when they are exposed to harmless products such as petroleum products and ethylene glycol (anti-freeze). The generation of false positives in civilian contexts is especially troublesome due to the potential for mass hysteria.⁷²

**Figure 6** M-8 Chemical Detector and Identifier Paper

Source: KI4U Incorporated

---

⁷² Institute of Medicine. Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response
The HAZMATCAD™, manufactured by Microsensor Systems Incorporated, detects and classifies CW agents like Phosgene (CG) or Hydrogen Cyanide (AC). The portable lightweight device, which uses Li-Ion batteries, is ideal for first responders.
Technical Underpinnings

The Institute of Medicine outlines the technologies used in chemical weapon detection devices. Excerpts of that information are provided below.

Table 9 Technologies Used in Chemical Weapon Detection

<table>
<thead>
<tr>
<th>Technology</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ion Mobility Spectrometry (IMS)</td>
<td>IMS technology is mainly used to detect nerve, blister, and blood agents in mobile detectors.</td>
</tr>
<tr>
<td>Fourier Transform Infrared Spectrometry (FTIR)</td>
<td>FTIR is a technique that can identify compounds that are separated by gas chromatography. FTIR detectors are used to detect a variety of CW agents.</td>
</tr>
<tr>
<td>Color-Change Chemistry</td>
<td>Many of these paper kits are complex and include multiple tests for specific agents or families of agents. Color change detectors can detect nerve, blister, and blood agents.</td>
</tr>
<tr>
<td>Electrochemical Sensors</td>
<td>Function by quantifying the interaction between an analyte's molecular chemistry and the properties of an electrical circuit. Electrochemical detectors are used in mobile detectors to detect blister, nerve, blood, and choking agents.</td>
</tr>
<tr>
<td>Flame Photometry</td>
<td>Since most elements will emit a unique and characteristic wavelength of light when burned in a flame, this device allows for the detection of specific elements. Flame photometric detectors are commonly used in gas chromatographs.</td>
</tr>
<tr>
<td>Thermoelectric Conductivity</td>
<td>Thermoelectric conductivity detection technology has only recently been applied to chemical agent detection.</td>
</tr>
<tr>
<td>Infrared Spectroscopy</td>
<td>When infrared radiation passes through a gas, absorption of radiation occurs at specific wavelengths that are characteristic of the vibrational structure of the gas molecules. Infrared detectors are used in mobile detectors to detect blister and nerve agent vapors.</td>
</tr>
<tr>
<td>Photoacoustic IR Spectroscopy (PIRS)</td>
<td>As in infrared spectroscopy, PIRS uses selective adsorption of infrared radiation by CWA vapors to identify and quantify the agent present.</td>
</tr>
<tr>
<td>Photo Ionization Detectors (PID's)</td>
<td>Operate by passing the air sample between two charged metal electrodes in a vacuum that are irradiated with ultraviolet radiation, thus producing ions and electrons. PID's are used in mobile detectors to detect nerve, blister, and mustard agents.</td>
</tr>
<tr>
<td>Surface Acoustic Wave (SAW)</td>
<td>Sensors detect changes in the properties of acoustic waves as they travel at ultrasonic frequencies in piezoelectric materials. Acoustic wave sensors are used in mobile detectors to detect nerve and blister agents.</td>
</tr>
<tr>
<td>Raman Spectroscopy</td>
<td>Based upon the observation that when radiation is passed through a transparent medium, chemical species present in that medium scatter a portion of the radiation beam in different directions. Raman spectroscopy appears not to be applicable for detecting CWA precursors and degradation products in soil samples but has applicability in air samples.</td>
</tr>
<tr>
<td>Mass Spectrometry (MS)</td>
<td>A sample is introduced into the instrument, a charge is imparted to the molecules present in the sample, and the resultant ions are separated by the mass analyzer component. Many mass spectrometers are specifically designed to detect various CW agents and have enormous applicability in detecting agents in most types of samples.</td>
</tr>
<tr>
<td>Gas Chromatography (GC)</td>
<td>Like mass spectroscopy, this method also offers high sensitivity and specificity in detecting CWA in many sample forms.</td>
</tr>
</tbody>
</table>

Source: Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response Institute of Medicine, National Academies Press
Biological Detection Technologies

Biological Weapons

According to a committee of medical experts convened by the Institute of Medicine, “the most probable course of events in a terrorist attack involving a biological agent is a covert attack that, after a period of hours to weeks, will result in victims widely distributed in time and location. Because these biological agents do not immediately produce effects, the first indication of an attack with a biological agent may be the recognition of an unusual distribution or number of cases of disease, long after the initial aerosol or solution has been dispersed or degraded.”

Therefore, the laboratory analysis of clinical sample by departments of public health, and the information technology networks they use to share information across jurisdictional boundaries, will play a crucial role in determining that a biological attack has occurred.

Microbial Detection – Research and Development

The detection of biological agents occurs in two stages involving: (1) a probe, and (2) a transducer. “Probe technology deals with how the assay or detection device recognizes the particular target microbe. Transducer technology deals with how the assay or detection device communicates the activity of the probe to the observer. Together, probe and transduction systems determine specificity, sensitivity, and time required to make an identification.”

Probe Technologies

Probe technologies include those based on: nucleic acids, antibody/antigen binding, and ligand/receptor interactions.

Transducers

Transducer technologies include: electrochemical, piezoelectric, colorimetric, and optical systems.

Figure 8 GeneChip™p53 Probe Array

Source: Affymetrix Corporation

73, 74 Institute of Medicine. Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response
Detection of Biological Agents in the Environment

“Real-time detection and measurement of biological agents in the environment is daunting because of the number of potential agents to be distinguished, the complex nature of the agents themselves, and the myriad of similar microorganisms that are a constant presence in our environment and the minute quantities of pathogen that can initiate infection. Few, if any, civilian agencies at any level currently have even a rudimentary capability in this area. A number of military units, most notably the Army’s Technical Escort Unit, the U.S. Marine Corps Chemical Biological Incident Response Force, and the Army Chemical Corps, presently have some first-generation technology available.”

Nuclear Weapons

High levels of radiation exposure can cause sickness or death. Since radiation can not be detected by the senses of smell, touch, sight, or feel, public safety personnel must be able to detect and measure dangerous levels of radiation with the appropriate equipment. Additionally, emergency personnel like nurses and EMTs must understand the relationship between the amount of radiation a person receives and the associated health effects.

There are basically three categories of radiation detectors:

- Rate (or sometimes called ‘survey’) meters
- Dosimeters
- Geiger Counters

Rate Meters

Rate meters measure radiation strength or the rate of radiation. Some meters operate specifically in low ranges, others in high ranges, while a third category are adjustable through a range of radiation strengths. Personnel who use rate meters must understand how rates of radiation are calculated.

Dosimeters

According to the Chemical Institute of Canada, “a dosimeter is a small, calibrated electroscope worn by laboratory personnel and designated to detect and measure incident ionizing radiation or chemical exposure.” Dosimeters allow the person wearing them to calculate how much radiation they have received since they began wearing it, as opposed to the rate of radiation they are currently being exposed to, which rate meters are designed to calculate.

Geiger Counters

According to NASA, “a Geiger counter usually contains a metal tube with a thin metal wire along its middle, the space in between is sealed and filled with a suitable gas, and with the wire at about +1000 volts relative to the tube. The instrument is called a “counter” because every particle passing it produces an identical pulse, allowing particles to be counted (usually electronically) but not telling anything about their identity or energy (except that they must have sufficient energy to penetrate the walls of the counter. Geiger counters count the decay rate of radiation. Specifically, they count both beta and gamma radiation.”

---

75 Institute of Medicine. Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response
76 Chemical Institute of Canada. http://home.nas.net/~dbc/cic_hamilton/dictionary/d.html
Emergency personnel will use decontamination/mitigation procedures to remove chemical, biological (bacteriological), and radioactive particles from various surfaces to make them harmless. If used promptly and appropriately, decontamination devices and agents can reduce to a harmless level the amount of radioactive, biological, and chemical contaminants on people, clothing, material, buildings and land.

**General**

In general, specific decontamination methods and agents are used for a specific kind of contamination. However, highly sophisticated decontamination devices can be used for radioactive, biological, and chemical decontamination all at once.78

**Federal Standards**

The DHS, through its ODP program, “is the focal point for providing support to State and local law enforcement agencies in the development of counter-terrorism technology and standards, including technology needs for chemical and biological defense.”79 To meet the needs of State and local emergency first responders, the Office of Law Enforcement Standards (OLES) at the National Institute of Standards and Technology (NIST), working with NIJ, the Technical Support Working Group (TSWG), the U.S. Army Soldier and Biological Chemical Command (SBCCOM), and the Interagency Board, has developed chemical and biological defense equipment guides. The Guide for the Selection of Chemical and Biological Decontamination Equipment for Emergency First Responders was developed to provide emergency first responders throughout the country with guidance in the evaluation and purchase of decontamination equipment.

Since the ODP is approving and funding almost all of the mitigation/decontamination training in the State through First Responder Equipment Grants administered by TEEX, the information from their guides is central to training in this area. Therefore, the following sections provide excerpts from the Guide for the Selection of Chemical and Biological Decontamination Equipment for Emergency First Responders that describe appropriate equipment and procedures.

**Overview of Chemical-Biological Decontamination**

**Decontamination Process**

“A decontamination process refers to a method employed to destroy, reduce, or remove a contaminant to an acceptable level. There are several methods used to decontaminate CB agents. These methods consist of physical, chemical, and thermal processes.

**Physical Processes**

“Physical processes are used to remove CB agents from surfaces. It should be noted that another means of decontamination would be necessary for CB detoxification. High-pressure systems, sorbents (simple inert), and solvent washes are examples of physical processes and are explained in the remainder of this section.

**Sorbents (Simple Inert)**

“Sorbent technology uses materials that physically remove liquid chemicals from surfaces (e.g., skin). Generally, synthetic sorbents adsorb liquids, and natural sorbents absorb them. An example of such equipment is the Decontamination Kit, Personal No. 2, Mark 1 (Figure 9), manufactured by Richmond Packaging Limited.

![Figure 9 Decontamination Kit, Personal No.2, Mark 1](source: Richmond Packaging Limited)

**Solvent Wash**

“The use of a solvent to remove a CB contaminant is a physical rather than a chemical process. Chemical agents are removed from a surface by washing the molecules away using water, alcohol, freon, diesel fuel, etc.

**High-Pressure Systems**

“Decontaminants, such as water and carbon dioxide, sprayed at high pressures are effectively used to physically remove chemical and biological agents from surfaces. Studies have demonstrated that chemical agents can be removed from surfaces with water pressures <3000 lb per square inch (psi). One example of decontamination equipment utilizing a high-pressure system is the K1-05 standard unit (Figure 10) manufactured by Alfred Karcher Gmbh & Company. The K1-05 system employs high-pressure carbon dioxide to physically remove contaminants.

![Figure 10 K1-05 Standard Unit](source: Alfred Karcher Gmbh & Company)
Chemical Processes
“Chemical processes involve the use of reactive or catalytic chemicals (sorbents) to neutralize CB contaminants. Another means of decontamination would be necessary for chemical agent, or biological agent removal. An example of decontamination equipment utilizing reactive sorbents is the Decontamination Kit, Individual Equipment: M295, manufactured by Truetech (Figure 11).

Figure 11  Decontamination Kit, Individual Equipment: M295

Source: TrueTech

Thermal Processes
“Thermal processes remove CB contaminants through vaporization. It should be noted that another means of decontamination is necessary for agent detoxification. An example of decontamination equipment utilizing a thermal process is the Karcher mobile field laundry CFL 60 (Figure 12) that both physically and thermally removes decontaminates.

Figure 12  Karcher mobile field Laundry CFL 60

Source: Alfred Karcher Gmbh & Company
Decontamination Applications

“The three application areas involved with CB decontamination are personnel, equipment, and infrastructure.

Personnel Decontamination

“Personnel decontamination refers to the ability to decontaminate CB agents from human skin and personal equipment (e.g., clothing, personal protective equipment) that may pose a direct threat to human health through direct contact. Decontamination of the skin must quickly and efficiently remove the contaminant without causing damage to the skin. Skin decontaminants can either destroy the contaminant on the skin through chemical or biological reactions or physically remove it from the skin.

Equipment Decontamination

“Equipment decontamination refers to the ability to decontaminate CB agents from the exterior surfaces of equipment. This includes the decontamination of both large (e.g., vehicles) and small items (e.g., computers, communications equipment). An example of this type of equipment is the Karcher MPDS multipurpose decontamination system (shown in Figure 13). The MPDS is equipped with a high-pressure spray system and depending on the decontaminant that was used, either chemical or mechanical technologies are employed.

![Figure 13 Karcher MPDS Multipurpose Decontamination Equipment](Source: Alfred Karcher GmbH & Company)

Infrastructure Decontamination

“Infrastructure decontamination involves the removal of CB agents from large-scale items (e.g., buildings, roadways). Due to their extensive surface area, these items require special consideration during the performance of decontamination operations.
CB Decontaminants

“Two types of decontaminants, physical and chemical, remove or reduce CB agent to an acceptable level. Physical decontaminants include water, hot air, weathering, Fuller’s Earth, and surfactants. Chemical decontaminants include oxidizing agents, and microemulsions.

Physical Decontaminants

“Physical decontaminants are substances used to remove CB contaminants from surfaces. Water, hot air, Fuller’s Earth, weathering, and surfactants are examples of physical decontaminants.

Water

“Water is used to physically remove CB contaminants from surfaces. Water with the addition of detergents is effective for the decontamination of surfaces and materials contaminated with CB agent. Decontamination by detergents and soaps in water occurs predominantly by the physical removal or dilution of agent. The use of soap and water for the physical removal of contaminants from skin and equipment will limit the spread of contamination.

Hot Air

“Hot air is used to physically remove CB contaminants from surfaces. The effectiveness of hot air decontamination varies with respect to the physical properties of the CB agent being decontaminated. For example, CB contaminants distributed over a nonporous or nonabsorbent surface are readily removed using heat. However, if the CB contaminants are distributed over a porous or absorbent surface, additional heat and time are required to fully remove it.

Fuller’s Earth

“Fuller’s Earth is a nonplastic form of kaolin that contains an aluminum-magnesium silicate. The decontamination process involved with Fuller’s Earth is the physical removal of the agent from surfaces. Crushed Fuller’s Earth is best suited for personal decontamination, such as removing CB agent from the skin of an exposed individual. At some point, the contaminated Fuller’s Earth will need to be subjected to a detoxification procedure.

Weathering

“Weathering describes a passive form of decontamination whereby natural sources of heat and UV radiation (sunlight), water (precipitation), and wind combine to decontaminate a vehicle, a piece of equipment, large structures, and large areas of terrain. During the weathering process, decontamination occurs by evaporation of the contaminant (physical removal) or destruction of contaminants by hydrolysis or, less likely, by photolysis (chemical reaction).
Surfactants

“There are three categories of surfactants currently in use: anionic surfactants, cationic surfactants, and nonionic surfactants. The intent of a surfactant is not to detoxify the CB agent but to solubilize it into a solution that can detoxify it. Anionic surfactants are generally more powerful in terms of solubilizing CB contaminants into an aqueous solution than cationic or nonionic surfactants.

Chemical Decontaminants

“Chemical decontaminants are substances used to neutralize CB contaminants. Most of the current decontaminants used in the detoxification of CB contaminants can be considered reactive chemicals. Reactive chemicals are ones that readily react with another chemical without the need for stirring, heating, or shaking.

Oxidizing Agents

“Powerful oxidizing agents, such as calcium hypochlorite (Ca(OCl)2) and sodium hypochlorite (NaOCl), are used effectively for the detoxification of CB contaminants.

Microemulsions

“Microemulsions are thermodynamically stable mixtures of water, oil, surfactants, and co-surfactants that appear macroscopically as a homogeneous phase. When a chemical agent encounters a microemulsion system, it is partially dissolved (partitioned) into the organic phase of the microemulsion. Once dissolved, the agent can react with the water-soluble decontaminant at the surface of the organic portion of the microemulsion.”

---

Background

A wide range of individuals and organizations can carry out attacks against critical information technology infrastructures. In the field of Homeland Security, the primary concern is the threat of organized “cyber attacks capable of crippling our Nation’s critical infrastructures, economy, or national security.”

A high degree of technical sophistication is needed to launch a devastating attack, and to a large extent, this explains why one has not been executed. However, evidence exists that hostile actors have exploited weak points in information technology architectures and gained access to systems where the potential for devastating attacks was possible. For example, according to Jim Williams, a former member of the FBI’s San Francisco computer-intrusion squad, there have already been attacks on the nation’s telecommunications, power, and emergency services systems that have risen to the level of an “immediate national security concern and response.”

Furthermore, a former director of a major intelligence agency, who requested anonymity, indicated that a classified 1997 “red team” exercise employing world-class network security experts (hackers) demonstrated the ability of a cyberattack to cripple the nation’s banking systems.

As President Bush’s National Strategy to Secure Cyberspace points out, adversaries of the US could carry out attacks on information networks for a variety of reasons. “In peacetime America’s enemies may conduct espionage on the Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping US information systems, identifying key targets, lacing our infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the nation’s political leaders by attacking critical infrastructures and key economic functions eroding public confidence in information systems.”

Security Tools

The National Information Assurance Partnership (NIAP) is a partnership that the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) established to meet their respective responsibilities under the Computer Security Act of 1987. The partnership, which was actually created in 1997, “combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for evaluating those products and systems.” Thus, NIAP interacts extensively with commercial and government entities to help set security standards for software and hardware that address challenges to the Nation’s critical information technology infrastructures. Based on guidelines issued by NIST and NIAP, network security administrators typically use a layered approach to secure their critical networks. The layered-security approach maintains...
appropriate security measures and procedures at five different levels within a network environment:

- Perimeter
- Network
- Host
- Application
- Data

Below, is a definition of each of these levels and an overview of the various security measures that operate on each. The aim is to provide a foundation-level understanding of network security.

**Decreasing a Network’s Vulnerability to Attack**

An important idea to network security administrators implementing layered security is the concept of “work factor.” Work factor is defined as the “estimated amount of effort or time that it will take a potential intruder to penetrate a network, or defeat a particular security counter-measure, when using specified amounts of expertise and resources.” Networks that have high work factors require a lot of effort to break into, while networks with low work factors can be broken into relatively easily. Hackers that determine a network has a high work factor, which is a benefit of the layered approach, are more likely to move on or try to break into networks that are less secure.

**The Layered-Security Model**

Table 10 presents the technologies that function at the different levels of the layered-security model. A more complete description of the technologies follows the table.

**Table 10 Levels of Security**

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Applicable Security Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Perimeter</td>
<td>Firewall&lt;br&gt;Network Based Anti-Virus&lt;br&gt;VPN encryption</td>
</tr>
<tr>
<td>2. Network</td>
<td>Intrusion Detection/Prevention System&lt;br&gt;Vulnerability Assessment Tools&lt;br&gt;Access Control/User Authentication</td>
</tr>
<tr>
<td>3. Host</td>
<td>Host Intrusion Detection System&lt;br&gt;Host Vulnerability Assessment&lt;br&gt;Anti-Virus&lt;br&gt;Access control/user authentication</td>
</tr>
<tr>
<td>4. Application</td>
<td>Host IDS&lt;br&gt;Host VA&lt;br&gt;Access control/user authentication&lt;br&gt;Input Validation</td>
</tr>
<tr>
<td>5. Data</td>
<td>Encryption&lt;br&gt;Access Control/User Authentication</td>
</tr>
</tbody>
</table>


**Level 1: Perimeter Security**

The perimeter is the “wall” between an organization’s network and the outside world (i.e., Internet). As such, it is the first line of defense against outside unauthorized users and acts as the first and last point of contact for security defenses protecting the network.

“The perimeter consists of one or more firewalls and a set of strictly controlled servers located in a part of the perimeter referred to as the DMZ (demilitarized zone). A DMZ typically contains the web servers, email gateways, network anti-virus, and DNS servers that are necessarily exposed to the Internet. The firewall enforces strict rules about who and what can have access to the network as well as rules about how servers in the DMZ can interact with the Internet and the inside network.”

The following technologies provide security at the network perimeter:

- **Firewall.** A firewall is typically installed at the edge of a network perimeter (see Figure 14) and generally performs three functions: (1) traffic control; (2) network address translation (NAT); and (3) VPN termination. Traffic control is performed by determining the source and destination of network traffic, both incoming and outgoing. The firewall ensures that only traffic permitted by its predetermined settings is allowed through. The firewall also translates internal IP addresses to IP addresses that the Internet can see. This translation protects critical information about the internal network architecture. Finally, a firewall can terminate VPN tunnels (see below).

![Figure 14 A Typical Firewall Installation](image)

*Source: Still Secure Corporation*

- **Network-based anti-virus.** NIST defines a computer virus as a “string of code that attaches itself to another computer program or document. Once it is attached it replicates itself by using some of the resources of the co-opted program or document to replicate and attach itself to other host programs and documents. Malicious code is not limited to viruses per se; other categories of malicious code include worms and Trojans. The impact of a virus, worm, or Trojan can be as harmless as a pop-up message on a computer screen, or as destructive as deleting all the files on a hard drive.”

  The purpose of network based anti-virus software installed in the DMZ is to compare incoming and outgoing email messages and network traffic to a database of previously identified viruses, worms, and Trojans. Network-based anti-virus software “quarantines” infected messages at the network level and notifies network

---


administrators and security personnel of a problem. Stopping infected messages at the network level prevents their entering and propagating across an entire network. Network-based anti-virus software works in conjunction with anti-virus software installed on individual servers and desktop computers. Anti-virus software is very effective as long as the database of known viruses, worms, and Trojans is updated frequently.

- **Virtual Private Network.** A virtual private network (VPN) employs high level encryption to create a secure communication channel between two devices that communicate information over a public network (e.g. the Internet). VPN tunnels can be terminated on any VPN enabled router, firewall, or server within a network’s DMZ. The use of VPN enabled connections on all of an organization’s remote and wireless network segments is a very important security practice.

### Level 2: Network Security

The Local Area Network (LAN) and the Wide Area Network (WAN) are components of the network level in the layered-security model. An internal network includes desktops, printers, and servers. In large, geographically dispersed organizations it may also include point-to-point frame relay connections. Once the perimeter of a network is crossed, traveling across the network is fairly easy.

The following technologies provide security at the network level:

- **Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).** IDS and IPS technologies “inspect all inbound and outbound network activity and identify suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.”

IDS and IPS devices analyze network traffic and identify patterns that are consistent with an attack that might compromise or allow unauthorized access to a system. IDS and IPS devices accomplish this task by comparing network traffic to known attack profiles. When the devices determine that an attack is occurring, they immediately take action. IDS tools alert the network security administrator that an attack has occurred; IPS tools actually block the malicious traffic. Typical IPS and IDS configurations are shown in Figure 15 and 16.

#### Figure 15 Intrusion Detection System

![Intrusion Detection System Diagram](image)

*Source: Still Secure Corporation*

---

Figure 16 Intrusion Prevention System

- **Network Vulnerability Assessment (VA).** “The purpose of an internal network vulnerability assessment is to perform an audit of network devices to identify possible security risks within the perimeter of a network.”90 In general, VA software maintains a database that identifies all of the known vulnerabilities for various network devices and applications. During an assessment, the VA tool tests network devices against these vulnerabilities. Upon completion of the assessment, the VA tool provides a report to the network security administrator which identifies the location and nature of the problems that were found. Additionally, the tool recommends immediate and long term solutions to the problem.

- **Access control/Authentication.** Access control refers to the procedures used to authenticate the identity and access rights of individuals who access a network. Access should only be granted to authorized users.

**Level 3: Host Security**

In the layered-security model, individual devices in the network like desktop computers, servers, routers, and switches are considered the host level. Each of these devices has configurable settings that can create security problems if they are set incorrectly. “These parameters include registry settings, services (applications) operating on the device, or patches to the operating system or important applications.”91

The following technologies provide security at the host level:

- **Host-Based Intrusion Detection System (IDS).** Host-based IDSs work in the same manner as network IDSs except that they monitor traffic on a single network device. “IDSs are installed primarily on servers, but also can be found on desktops and laptops. While network-based IDS software inspects packets on the network for suspicious activity, host-based IDS software monitors system files, processes, and log files for suspicious activity.”92

- **Host-Based Vulnerability Assessment (VA).** These tools perform vulnerability assessments on a single network device.

- **Anti-Virus.** Anti-virus tools are installed on individual desktops and servers. They work in conjunction with network-based anti-virus software.

---

• **Access control/Authentication.** Access control refers to the procedures used to authenticate the identity and access rights of individuals to a single network device (e.g. a desktop). Access control measures at the host and network level are interconnected.

**Level 4: Applications Security**

“Application security is one of the most challenging aspects of network security. In simple terms, application-level security ensures that applications interact with end users only in ways that were intended by the application’s developers. Application-level security is focused on preventing the unauthorized use of an organization’s information by hackers attempting to gain access to the network directly through the application itself. Application-level hacks typically exploit weaknesses in HTML coding, Common Gateway Interfaces (CGIs), or in third party products such as web servers or scripts.”

The following technologies provide security at the application level:

• **Application Shield.** The application-layer firewall is commonly referred to as the application shield. These products are often installed on web servers, email servers, and database servers. They are programmed to “understand” or learn typical application behavior. “For example, an application shield on an email server would likely be configured to prohibit an incoming mail message from automatically launching executable files, because that is not a typical or necessary email function.”

• **Access control/Authentication.** Application shields are closely connected to the application they are shielding. Therefore, they produce an extra layer of user authentication, as well as traffic verification.

• **Input Validation.** “Interactions between people and a user interface can produce input errors or be exploited if proper security measures are not used. Input validation verifies that application input traveling across a network is safe to process.” If any input elements are altered during a user session or additional character types are injected, the tool stops the alteration from occurring and possibly warns an administrator of the anomalous behavior. For example, consider a Web-form with an area code field. The only acceptable input from this field should be three characters, digits only. Any other inputs should be rejected.

**Level 5: Security at the Data Level**

Data-level security is a combination of organizational policies and encryption. The best way to shield sensitive data on a network against unauthorized access or tampering is encrypting data where it is actually stored in case all other security measures fail. Additionally, organizations should have clearly understood and followed policies that detail who has access to certain information, what they can do with it (i.e. read only), and who has ultimate responsibility for its security and integrity.

• **Encryption/Decryption.** “Data encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Data decryption is the process of converting encrypted data back into its original form. There are many types of data encryption, and they are the basis of network security. Common types include Data Encryption Standard and public-key encryption.”

---

Background

In this section we will review the principles behind the technologies developed for detecting explosives. The two major categories of mature technologies for this purpose are X-ray and neutron transmission based. Another technology is trace detection, or chemical sniffing.

X-ray Based Technologies

X-ray systems and sources have benefited from years of development. They were initially used for medical imaging and then found application in luggage inspection and non-destructive testing systems in the electronics and other industries.

Scientific Underpinnings

The explosives-detection technologies that are based on X-ray techniques measure the X-ray attenuation of the materials that make up the item being scanned. Compton scattering and the photoelectric effect are the primary mechanisms responsible for X-ray attenuation in materials at the energy ranges used by explosives-detection equipment.\(^\text{97}\)

Figure 17  X-ray systems, luggage inspection.

The National Academy of Science document *Practicality of Pulsed Fast Neutron Transmission Spectroscopy for Aviation Security* describes the operation of these devices in the following way:

“The photoelectric effect results in X-ray absorption, whereas Compton scattering merely scatters X-rays, altering the path and energy of the scattered photons (X-rays). The significance of the photoelectric effect is greater for materials composed of elements with a high atomic number (Z), such as metals or other inorganic materials. However, this significance drops off rapidly with increasing X-ray energy. For organic materials (low Z), Compton scattering is the dominant X-ray attenuation process, and it varies with less X-ray energy. Comparing attenuation measurements at different X-ray energies will therefore allow for distinguishing materials from another. For example, inorganic materials can be

identified by rapidly changing X-ray energy, whereas organic materials will display a more subtle change. Multienergy X-ray based detection equipment have been developed and are suitable for distinguishing organic and inorganic materials and for semiquantitative density measurements.  

Airport Scanning

Airports have begun to use computerized tomography (CT scanners), a more sophisticated form of X-ray scanning, to screen passenger luggage for explosives. These devices “fire X-rays into baggage with circular arrays of emitters and detectors rotating around bags passing along a conveyor belt.” Using CT, three dimensional images of items inside a luggage can be created. “The ability to reconstruct two-dimensional cross-sectional images (tomographs) and then full three-dimensional volumes can greatly improve the ability to determine explosive threats by identifying certain shapes or patterns, such as wires, batteries, or detonators, as well as measure the volume of the material in question. The additional geometrical information supplements the material x-ray attenuation information and results in a more specific discrimination of explosive materials.”

Figure 18 3DX-6000 Full Volume Computer Tomography Scanner

The FAA has certified four EDSs, all of which are X-ray based CT systems, for service in the nation’s airports. Three of the machines, the CTX-500, CTX-5000 SP, CTX 550DS are manufactured by In Vision Technologies. A fourth system, the 3DX-6000, is manufactured by L3 Security and Detection Systems.

Cargo Scanning

L3 Communications Inc. manufactures several cargo scanning systems, including a 450 KeV system, which they claim is capable of 4 inches of steel penetration. Most cargo containers have a 1/8 inch thick steel shell, so 4 inches would appear to be adequate for any inspection. However, the amount of power needed for a cargo application depends on the contents of the cargo. In applications that involve inspecting empty containers, low energy neutron devices can prove more effective.

98 National Academy of Science. The Practicality of Pulsed Fast Neutron Transmission Spectroscopy for Aviation Security
Bio-Imaging Research Inc (BIR) is developing mobile cargo scanning systems that can be easily redeployed, both within a single port facility or between several different ones. Mobility at a port facility is a requirement because it is often impractical to commit a single area of a port to a scanning facility.

Figure 19  BIR dual head 9 MeV systems take top and side images of cargo containers at Japanese Seaport

The private, 35-employee Advance Research and Applications Corp. (ARACOR) recently won a $40 million dollar contract to sell eight of its mobile ARACOR Eagle cargo inspection systems to the U.S. Bureau of Customs and Border Protection. The Eagle operates at 6 MeV and can produce images of items beneath 12 inches of steel. Since early 2001, there has been an Eagle in operation at the Port of Miami.

ARACOR, L3, and BIR are major providers of X-ray cargo inspection systems. Other manufacturers include OSI in Hawthorne, Calif., and Heimann Systems in Wiesbaden, Germany. These systems typically use linear accelerators from Varian in Las Vegas, Nevada, as the X-ray source to produce energy levels in excess of 1 MeV.

Neutron Transmission Based Technologies

Scientific Underpinnings

“Gamma ray systems use radioactive isotopes or pulsed fast neutron (PFN) sources to show structural information inside luggage or containers as well as the elemental make up of the materials inside. Two basic techniques utilizing neutrons are used in this kind of explosives detection equipment: (1) fast and thermal neutron activation and (2) fast neutron transmission. Gamma ray systems, although less developed than X-ray systems, can also detect nuclear materials a differentiation that X-ray systems alone cannot make.”

“Fast and thermal neutron activation uses a neutron source to generate the nuclear reaction of a neutron with the nuclei of nitrogen, carbon, and oxygen, which produces gamma rays and...”

---

at specific energies. By detecting and identifying the energy of these gamma rays, one can then determine the amount of those elements in the probe material. Using single-photon imaging techniques similar to medical application, one can then generate a two-dimensional image of the luggage. Neutron sources can be reactors (fast neutron activation) or radioactive isotopes (thermal neutron activation).

“The neutron transmission and scattering methods make use of the specific material, and energy-dependent absorption and scattering cross-sections of neutrons interacting with the nuclei of different elements. They can be used to determine hydrogen, carbon, nitrogen, and oxygen content in an object. Due to the nature of the neutron interaction with the probe nuclei, radioactive activation of some luggage content may result.”105

**Cargo Inspection Systems**

Science Applications International Corp. (SAIC) in San Diego offers a mobile cargo scanning system that uses gamma rays to image the contents of cargo containers. Because of their energy level, these gamma rays are able to penetrate 6 inches of steel; far less than the 12 inches of penetration that can be provided by high energy X-ray systems. Due to their enhanced penetration depth, high energy X-ray systems are capable of scanning cargo at 1 foot per second, which is much higher than the 1 inch per second capability of SAIC’s system. However, SAIC’s lower energy level gamma ray systems require a significantly lower amount of shielding to protect operators from high-energy, linear accelerator based X-ray systems. “Cargo inspection systems operating at 6 MeV and above require many tons of shielding, which can increase system costs and preclude relocatable systems that can be transported on the bed of trucks.”106 A SAIC mobile gamma ray system, the VACIS3, is deployed at 30 U.S. water ports. The VACIS3 produce a gamma ray that can create images of explosives, weapons, drugs or other contraband through 6 inches of steel.

![Figure 20 Mobile Vehicle and Cargo Inspection System (Mobile VACIS)](source: SAIC Cargo Inspection Group)

---

OSI Systems Inc. of Hawthorne, Calif., offers a pulsed fast neutron analysis (PFNA) gamma ray system that creates a 3D scan of a cargo container. The scan, which is created using two orthogonal pulsed neutron sources, includes 3D structural information and a chemical composition analysis of the objects stored within the container.\textsuperscript{107}

**Tracing Molecules Of Explosive Materials**

Another kind of explosive detection technology, trace detection, identifies residual chemicals on the surface of luggage, clothing, packages, and bags. If someone touches a material, minuscule amounts of the material will become attached to their bodies or personal items like bags and packages. The goal of trace detection devices is to identify explosive materials amongst these collected materials. Trace detection is usually employed as a second level of testing when the results of an x-ray scan indicate that explosives might be present. Although trace detection raises the level of certainty about the presence of explosives, its accuracy is still less than 100%.\textsuperscript{108}

**Scientific Underpinnings**


“Current trace detection technology, in use at airports and government facilities around the country, is called ion mobility spectrometry or IMS. In IMS a technician wipes a swab across a bag or a person’s clothing and collects trace materials of all kinds. Next, the technician places the swab into a machine the size of a desktop computer. The machine heats the sample to a temperature of approximately 200-degrees Celsius and vaporizes particles collected on the swab. Next, a radioactive source such as Nickel 63 subjects the vapor to a stream of beta particles. The beta particles collide with molecules in the vapor and knock electrons out of their orbits. Molecules without enough electrons are called ions, and this process is called ionization. A strong electrical field will also ionize molecules, and some trace detection systems use this method.

“The ions then flow into and through a 4-inch-long tube, called a drift tube. The system measures the length of time it takes various ions to make it all the way through the tube. All materials have a specific atomic weight. Heavier ions move more slowly than lighter ions. Scientists know how long it takes ionized molecules to travel through drift tubes. Government security departments maintain classified lists of explosive materials and their ionized characteristics. So when a trace detection machine at the entrance of, say, the FBI building in Washington, D.C., discovers an ion traveling at that speed of a particular plastic explosive ion, the system will alarm, and officers will investigate further.

“Trace detection equipment also comes in three forms. First, desktop-sized analyzers fit on small carts that can be wheeled through facilities. Second, there are hand held “sniffers,” appropriate for applications where space is limited. Third, there are walk-through portals that send a puff of air from the floor of the machine to the top. The air puff sends traces into a trap set on top of the portal, and the trap feeds materials into the detector itself. Major manufacturers include Ion Track Instruments of Wilmington, MA and Smiths Detection (formerly Barringer Technologies) of Warren, NJ.”\textsuperscript{109}


Trace Detection Challenges

One of the challenges that trace detection presents is its tendency to produce false alarms. For example, “one form of nitroglycerin is used in explosives, while another is used in heart medications. Both will alarm a conventional IMS system.” Manufacturers are developing new means, including mass spectrometry, to detect explosives with more accuracy and lower the amount of false alarms. Mass spectrometry measures the weight of ions, instead of the speed of ions in a drift tube.

Next Generation

Manufacturers are currently exploring technologies that will increase and refine the capabilities of explosive detection equipment.

Many believe that a technology, called Quadrapole Resonance or QR, may meet this challenge. QR, which was originally developed by the Department of Defense to detect land mines, uses radio waves to detect the presence of explosives. The device works by transmitting radio waves through an object. “When the radio waves pass through an explosive material, the molecules of that material will polarize or develop a small electrical charge. As the molecules lose their charge, they emit a very weak radio frequency signal that can be picked up and analyzed to detect explosives.”

The technique relies on radio waves. Therefore, equipment built using this technology would not require the same kind of expensive radiation shielding that x-ray and gamma systems require. While QR is considered very promising, X-ray, gamma ray and trace detection technology will continue to dominate the explosives detection landscape in the near future.

Background

According to the Nation’s Homeland Security Strategy, critical infrastructure and key assets represent targets whose destruction would “cause large-scale injury, death, or damage to national prestige.”[^112] Although these assets in and of themselves aren’t critical to the delivery of services on a national scale, their destruction could produce significant loss of life and/or economic and public health/safety consequences. Facilities in this category include nuclear power plants, electrical utilities, dams, and hazardous materials storage facilities. Other assets, include national symbols, monuments, and historical attractions that are symbols of the nation’s values or political and economic power. As one can see from Table 5, The Protection Challenge, in Part One, protecting America’s critical infrastructures and key assets represents an enormous challenge. First of all, our Nation’s critical infrastructures and key assets are highly complex, interdependent, and heterogeneous. Therefore, there are many “high value” targets that are attractive to terrorists. Secondly, ownership of these key assets varies. A significant amount of critical infrastructure, like dams and nuclear power plants, as well as institutions that have important symbolic value, are controlled by private institutions.[^113]

Given the number and kinds of potential targets, it is not practical to protect them against every kind of attack. As protective measures for specific kinds of attacks are developed, terrorists will revise their attack signatures.[^114] Any successful plan to protect critical infrastructure and key assets must be cognizant of these realities. Therefore, in this section, we focus simply on the basic building blocks of protection that are applicable to a wide range of physical assets.

Peripheral Security

This area is the most vulnerable one in a protection plan. The peripheral security measures against known threats will encompass the following systems:

**Smart Fence System.** Intrusion detection, perimeter viewing (Video Surveillance), long range viewing capabilities (RF, Radar, etc) are components of Smart Fence systems. These capabilities are combined with alarm systems and building access control systems.[^115]

SecurityGateway.com[^116], a source of security industry news and information, provides this list of technologies that underlie an effective “Smart Fence” (intrusion detection) system:

- **Sensors.** “Sensors are located around an asset and detect different types of activity. Sensors send signals to a control panel via wireless radio transmitters or via wires when there is a break-in attempt or unauthorized entry. Several types of sensors have been designed especially for intrusion detection:
  - **Motion Sensors.** Motion sensors detect movement in the area of coverage.
  - **Magnetic Contacts.** Magnetic contacts usually protect doors and windows. They send signals to a control panel when a door or window is being opened when the system is armed. They can also be used for detecting the removal of high-value objects and at other key points.

[^112]: National Strategy for Physical Protection of Critical Infrastructures and Key Assets Released by White House February 14, 2003
[^115]: Homeland Security: Critical Infrastructure Security

• **Glassbreak Sensors.** Glassbreak sensors protect windows, sliding glass doors and skylights and come in three variations: shock, acoustic and combination.

• **Shock Sensors.** Shock sensors “feel” the shock frequency wave produced by breaking glass and signal an alarm.

• **Acoustic Sensors.** Acoustic sensors “listen” for the unique sound of glass breaking.

• **Combination Sensors.** Combination sensors detect multiple activities before signaling an alarm.

• **Control Panel.** The control panel receives information from the sensors, processes it, and activates the alarms. Audio and/or visual indicators, such as bells or strobe lights, are set off. Encoded signals can also be sent to a central station, reporting exactly what occurred in precisely which area of the building.”

**Figure 21 Control Room**

![Control Room Image](image)

*Source: Professional Engineers and Geoscientists of British Columbia (Canada)*

- **Video Surveillance.** “Digital video surveillance and closed-circuit television (CCTV) equipment offers an efficient, effective way to monitor people and property. A video surveillance system integrated with a passive intrusion detection system allows staff to keep watch on multiple areas of a facility, or multiple facilities, from a single monitoring location. New thermal imaging systems detect both people and objects through bad weather, smoke, darkness, and other vision obscurants.”

- **Long Range Viewing (Radar, RF).** The Institute for Telecommunication Sciences defines radar as “a radio detection system that transmits short bursts (pulses) of rf energy and detects their echoes from objects (targets) such as aircraft or ships. The round-trip propagation time for the echo return may be used to determine the target’s range (distance from the radar’s antenna). If the transmitting antenna has a narrow beam (the usual case), the azimuth or elevation of the target may also be determined. Radar can be used to locate and track intruders before they reach the perimeter of a critical asset.”

---


• **Perimeter Patrol.** Unmanned Aerial Vehicles (UAV), fitted with sensors and/or video and infrared (thermal) capability, can be used to detect intruders, equipment, and CBN agents.

• **Camouflage.** The act of disguising an asset can be a major deterrent to preventing unauthorized persons from entering a protected space.

**Figure 22  Unarmed Aerial Vehicle – US Navy Drone**

Source: United States Navy

**Access Control and Internal Security**

Controlling who has access to a critical asset is an extremely important part of a security plan. The access control/ internal security system must be active and contain several layers.

• **Smart Access Control System.** An effective access control system must not only control authorized access to key assets, but must do it in a way that does not unduly impede the flow of people and goods. A technology that can be used to control access is the smart card, a credit card containing a secure microprocessor. Smart cards are already in wide use as “token systems” in public transportation facilities.

**Figure 23  Contactless Smart Card Reader at Washington D.C. Subway Station**

Courtesy: Washington Metropolitan Area Transit Authority
• **APL – Automatic Personnel Location and Management.** “A tag system can provide adequate security information on both local and guest employees to prevent any penetration of unauthorized personnel.”

• **Visitor screening.** Biometric identification incorporated into the internal security system provides additional important data on visitors and guest workers prior to offering them access to critical infrastructure. A biometric identification of such persons could be compared to terrorist databases, for example.

• **Wireless Communication.** Wireless communication systems linked to the central control panel allow for communication between security personnel at all times.

• **Smart image controls.** “This video based system provides security management by exceptions for both people and equipment. Any odd occurrence viewed or detected by the system will provide adequate alert information for security breach procedures.”

### Multi-Level Detection Systems (Weapons and Explosives)

These systems should provide the necessary alert against weapons and explosives. Such systems are employed in high value targets with frequent unknown visitors (federal buildings, national monuments, etc).

• **Metal Detectors.** “Walk-through metal detectors or magnetometers use magnetism to search for weapons with metal components. A handheld metal-detecting wand works the same way, by sending out pulsed magnetic fields that expand, contract, and create eddy currents that vary in value when a metal object gets in the way. The walk-through detector alarms when it finds metal on a person. The wand, using a smaller field, alarms when it finds metal in a person’s pocket or shoe. By dialing the circuitry up and down, operators can control the sensitivity of the magnetometer to detect smaller and larger metal objects. The shortcomings of magnetometers are obvious. If the sensitivity is decreased, small metal weapons, such as pocket knives, might go undetected. If the sensitivity is increased, detectors will detect non-offending metal objects, thus creating a false alarm. Similarly, the equipment cannot detect plastic or ceramic materials that can be used to make weapons or find an explosive made of non-metallic materials. However, viewed as one line of defense, walk-through metal detectors do what they are designed to do: detect metal and suggest further examination by security officers.”

• **X-Ray Body Scanners.** “In the search for weapons or bombs hidden on people, X-ray images are more revealing, and faster, than a beeping magnetometer. For several years, the U.S. Customs Service and federal and state correctional systems have employed X-ray body scanners to screen people for weapons as well as narcotics. Body scanners direct a low dose of X-ray energy at a person standing in front of a refrigerator-sized machine. The X-rays scan the person from head to toe, penetrating clothing and reflecting off the skin and any solid objects underneath the clothing. Detectors inside the equipment pick up the reflected X-ray energy, digitize this energy, and create an image.

---

on a monitor. The image will show ceramic and plastic weapons as well as other objects with significant density and mass. Body scanners may eventually become an adjunct to walk-through metal detectors at entrances to secure facilities. Before applying the technology widely, however, a civil rights issue must be considered. By penetrating the clothing, body scans create revealing images of people. Some observers call these scans electronic strip searches.  

Figure 24 X-ray Metal Detector Image

![X-ray Metal Detector Image](image)


• **Conventional X-Rays.** Conventional X-ray technology (see Concealed Explosives section) is used to screen packages and briefcases carried by people into government buildings or onto airplanes. “Conventional X-ray machines use conveyor belts to move bags and packages through an X-ray field. The system generates an image of items inside a bag or package. Because some materials react differently to X-rays than others, these systems generate images in different colors to help operators distinguish between organic and inorganic materials. While the appropriate colors will prompt X-ray machines to activate alarms, the technology relies largely on the knowledge and experience of the operator, who may question shapes and colors undetected by the system.”

Background

The mission of the Department of Homeland Security is to prevent terrorist attacks within the United States. An essential element of this mission is the interconnection of multiple federal agencies in a manner that allows them to sift through vast amounts of “unstructured” raw data (field reports, collection summaries, immigration records, Web page content, emails, open source news feeds) and infer, gather and share immediate, actionable intelligence. To carry out these duties, our Nation’s intelligence agents will use advanced information technology tools that allow them to quickly analyze unstructured data in its original language, organize it, eliminate what is useless, and present useful intelligence to those who must act on it. As President Bush noted at a speech at FBI headquarters, “We’re going to use the best information technologies to make sure information flows from this data bank of information to law enforcement officials.”\textsuperscript{125} Some of the advanced tools that President Bush was referring to include data warehousing, data mining, link analysis, and text mining.

Data Warehousing

Organizations collect huge amounts of data that contain valuable information about their operations. Unfortunately, much of this data is stored in databases that are heterogeneous in design and use. For a variety of technical reasons, the heterogeneous nature of these databases makes it hard for users to query information from them in a way that gives them a comprehensive view of their organizations operations. Data warehouses can help eliminate this problem by bringing together data from disparate databases into one data architecture so that users can use the information more effectively.

In the intelligence field, “the purpose of a data warehouse is to create a multidimensional picture of an individual by combining data from several different databases (DHS (INS), FBI, NSA, etc.) in order to gain a comprehensive view of the individual’s identities, values, and behavior.”\textsuperscript{126} The data warehouses will include information about bank and money transfer transactions, airline ticket purchases, automobile rental records, enrollment and graduate information from schools, credit card purchases, and records describing travel to and from the United States.

The construction of these super data warehouses will involve government contracts with large software and hardware firms like IBM, Oracle, and Sun as well as system integrators like Lockheed Martin, Northrop Grumman, and Raytheon. Additionally, commercial firms that provide demographic information, such as Acxiom, ChoicePoint, Experian, Polk will be involved.


Data Mining

Data mining is a method of extracting important trends and behaviors from data using automated analysis. It has been identified as the key technology in the battle against terrorism because it automates the manual process of searching and discovering knowledge in large data warehouses. For example, it can be used to “dig” through data and identify persons and/or activities associated with suspicious activities (inclusion on immigration “watch-lists,” suspicious overseas money transactions, etc).

This example illustrates how the data mining process works:

The users of a data mining package define which variables are the inputs and predicted outcomes and the software produces a model that relates inputs to outcomes. Machine learning software can then comb through a database and generate decision trees (IF/THEN) rules which an analyst can use to gain information about the characteristics of terrorists:

If Characteristic A <= X
AND Characteristic B >= Y
AND Characteristic C >= Z
THEN Terrorist Probability 80%

Data mining has been used over the years to discover hidden patterns, profiles, and signatures in large databases. However, using current data mining technology for homeland security is not practical because most current data mining approaches (IBM, Sybase, SAS, SPSS, Teradata,) look for patterns in a single database. Obviously, this is a problem in the area of homeland security because pertinent data will probably reside in a multitude of large, dynamic, distributed, heterogeneous databases “owned” by different agencies with disparate responsibilities. Recently there have been advances in data mining which could overcome this problem:

Figure 25 The Evolution of Data Mining

Source: “Data Mining for Homeland Security” Jesus Mena 2003

127 Mena, Jesus. "Data Mining for Homeland Security."
"Distributed" Data Mining

Data mining for homeland security and criminal detection will require a vast array of information gathering machine learning agents. As pointed out above, this is due in part to:

- Databases that are distributed by geography and stewardship.
- The scaling of extremely large databases.
- Heterogeneous data schemas and database architectures.
- Dynamic real-time data warehouses that are constantly being updated.
- Privacy and security issues which prohibit the movement of the data.

All of these factors make the movement of massive databases to centralized data warehouses for data mining for homeland security a huge challenge. Therefore, one goal is to “effectively mine heterogeneous data that is located in distributed sites so that networks can share the data – where the sum of the information is much greater than the parts. In a distributed homeland security system, agencies can exchange information with each other, intelligence such as perpetrator profiles can be created and distributed instantly.” Since agencies connected to the network can share information with each other, security and law enforcement agencies can construct profiles of terrorists instantaneously without moving the data, thus ensuring privacy, ownership and security at a much lower cost than building monolithic data warehouses.

To understand how this type of data mining system works, imagine a border crossing system in which machine learning agents are used to mine remotely, multiple databases such as Immigration, Department of Motor Vehicles, and demographics simultaneously without moving any of the data; only pointers to the results would be communicated, encrypted, and compressed to a centralized “mediator” agent. This type of remote data mining system incorporates the results of multiple distributed databases to detect potential terrorists at a point of entry border crossing. (See Figure 26) Two companies, InferX and InfoGlide currently provide this kind of technology.

Figure 26  Networked centric data mining for homeland security

Source: “Data Mining for Homeland Security” Jesus Mena 2003

The networked approach to data mining has applications not only in intelligence gathering and law enforcement but also in the commercial world for applications like fraud detection and business intelligence.\textsuperscript{130}

**Information Sharing**

Several companies have begun to provide enterprise information integration software that allows unified access to data that is exchanged between multiple, heterogeneous database systems and architectures. The technology reduces the time and cost associated with creating a unified view of information that exists in multiple diverse data environments. Providers of this type of information sharing technology include, Informatica’s Power Analyzer, and BEA Systems’ Liquid Data. IBM, through their DB2 Information Integration Data Joiner, and Oracle (Materialized Views) are also providing the ability to integrate their databases with those of others. Other firms such as Semagix and Data Junction are also providing the ability to integrate data from different database architectures. One unique application is System Research and Development’s (SRD) “Anonymous Entity Resolution” technology which allows investigators to determine whether a terrorist suspect appears in two separate databases, such as a terrorist watch-list and a car reservation system. “SRD software not only sifts through entity identification information like names, phone numbers, and addresses in separate databases but most importantly it scrambles and encrypts the information using a one-way hash function, which converts the name into a character string that serves as a unique identifier much like a fingerprint. Of course there is one drawback with this name matching system – a terrorist will probably use a series of aliases and fake addresses.”\textsuperscript{131}

**Link Analysis**

Law enforcement agencies, including the FBI, use link analysis software to identify terrorist networks and hierarchies. This software is used to understand how terrorist and criminal networks use communication systems, raise and transfer money, and to determine the sequence of various events and occurrences. “Link analysis is the first level by which networks of people, places, organizations, vehicles, bank accounts, telephone numbers, e-mail addresses, and other tangible entities and events can be discovered, linked, assembled, examined, detected, and analyzed.”\textsuperscript{132} Analysts and investigators often use link analysis software to answer such questions as “who knows whom and when and where have they been in contact?” The leading providers of this type of programs are The Automated Tactical Analysis of Crime (ATAC), i2, CrimeLink, Crime Workbench, NetMap, Orion and VisuaLink.

\textsuperscript{130,131,132} Mena, Jesus. “Data Mining for Homeland Security.”
Text Mining

Another key technology for homeland security is that of text mining, which allows investigators and analysts to sort, organize, and analyze gigabytes of unstructured free-form text during their inquiries. Text mining tools work with multiple languages making them ideal for agencies such as the CIA, FBI, and Department of Homeland Security which gather intelligence from sources all over the world.

Some of the major methods of text mining include feature extraction, clustering, and categorization.133

- **Feature Extraction.** The mining of text within a document in the attempt to find significant and important vocabulary within a natural language text document. For example, feature extraction can be applied to search and locate names or key terms such as “anthrax” or “bomb” used in e-mails, wireless phone calls, faxes, instant messages, chat rooms, etc.

- **Clustering.** The process of grouping documents with similar contents into dynamically generated clusters. Such technology could be used to automatically cluster key “homeland security” related concepts from thousands of documents, e-mails, Internet survey forms, phone and cellular records, and other communications for monitoring potential terrorists.

- **In Text Categorization.** Documents that belong to pre-determined categories are fed into a “trainer,” which generates a categorization scheme. When the documents are introduced into a categorizer, which incorporates the categorization scheme, the categorizer will then assign documents to different categories based on the taxonomy previously generated. These features are incorporated in programs such as IBM’s Intelligent Miner for Text.

Most text mining tools and techniques use all or some of the following processes:

- **Natural Language Processing.** Capturing critical features of a document’s content based on the analysis of its linguistic characteristics.

- **Information Retrieval.** Identifying those documents in a large collection of records that match a set of criteria.

- **Routing and Filtering.** Automatically delivering information to the appropriate destination according to subject or content.

- **Document Summarization.** Producing a compressed version of a large number of documents or collection of text, such as e-mails, with an abstract of their content.

- **Document clustering.** For grouping textual sources according to similarity of content, with or without predefined categories, as a way of organizing large collections of documents.

Private industry has been using text mining technology to organize the massive amounts of internal text documents they create on a daily basis within their organizations. Police departments are beginning to use the software to construct and organize criminal profiles. Some of the providers of text mining technology include Inxight www.inxight.com, Autonomy, and Convera.

---

133 Hsu, Jeffrey. “Critical and Future Trends in Data Mining: A Review of Key Data Mining Technologies/Applications.” 2003
Phenomenal Data Mining

Phenomenal Data Mining focuses on the relationship between data and the phenomena that are inferred from the data. For example, its advocates believe that it might be possible to examine a person’s travel history (visa records) or bank transactions and identify various characteristics of that person (terrorist?, business traveler?). However, to infer phenomena from data, the mining tool must have access to some facts about the relations between the data and their related phenomena. This could be included in the program that examines data for phenomena or in a knowledge base that can be created during the data mining process, but creating such a knowledge base involves embedding common sense into a database, which has proven to be a difficult task so far.134

Spatial and Geographic Data Mining

A huge amount of spatial and geometric data generated by barcode reading, remote sensing, satellite telemetry, etc., is collected in large databases. A significant amount of this data is image oriented and can represent a great deal of information if properly analyzed and mined.135

Analyses of spatial and geographical data includes such tasks as understanding and browsing spatial data, and uncovering relationships between spatial data items (and also non-spatial and spatial items). Spatial data mining is useful in the field of Homeland Security in such areas as Geographic Information Systems, remote sensing (WMD detection), cargo tracking, navigation, and intelligence (movement of terrorists and terrorist camps).

Figure 27  Satellite Image of University of California - San Diego Campus

Source: University of California – San Diego

---

General

The destruction of the World Trade Center Towers on September 11, 2001 alerted the nation and, indeed the world, to the dangers of terrorist attacks. As a result of this event, a number of federal programs were initiated, the most expansive and comprehensive being the establishment of the Department of Homeland Security (DHS). Although the stated mission of DHS is quite extensive, for the most part the various agencies gathered under the Department’s umbrella remain essentially intact and have essentially the same missions and responsibilities as before the reorganization. Moreover, funding for these subordinate agencies will, for the most part, continue to go to these respective agencies. Based on information distributed by DHS and other Homeland Security related federal agencies, it appears that employment opportunities for community and technical college graduates will fall chiefly into seven areas:

- Identification
- Network Security
- Weapons of mass Destruction (WMD) Detection
- WMD Mitigation and Decontamination
- Explosive Detection
- Critical Infrastructure Security
- Pattern Analysis/Data Warehouse Administration

Of these areas, Network Security, Data Warehouse Administration, and Critical Infrastructure Security, appear to offer the most potential for attractive employment opportunities for college graduates. Identification and Concealed Explosive Detection also have some employment attraction.

Types of HS Employment

Employment opportunities for college students can be classified into four categories:

- Service personnel
- Equipment specialists
- Inspectors
- Planners

**Service personnel** will be engaged in jobs such as policemen, fire fighters, nurses and nurses aides, guards, and equipment operators, e.g., airport screeners. In most of these cases, HS responsibilities will be only ancillary to the position’s overall responsibilities. Therefore, for the most part, these positions will require only a limited amount of special, HS related training and education. In general, the pay scales and other incentives for HS trained personnel will be little different from other people in the field without this training. However, people who receive formal certification in selected HS areas may be recompensed accordingly.

**Equipment specialists** will require the KSAs necessary to produce, install, calibrate, maintain, and repair HS related equipment. Although such equipment will often be similar to equipment employed in other areas, in many cases it will be quite different. To the extent that the equipment is unique, pay scales for skilled graduates will be very attractive.
Inspectors will be responsible for ensuring that regulations are followed, standards maintained, and proper protocols followed. Typically, inspectors will require considerable skill and experience and will be compensated accordingly.

Planners will be responsible for analyzing vulnerabilities, developing HS programs and protocols to address these vulnerabilities, and for updating these programs and protocols as necessary. Planners will not only require extensive knowledge of HS equipment and procedures, but also will have to have sufficient imagination and knowledge of terrorists’ approaches to determine changing HS needs as new situations arise. These positions are more likely to require bachelor or graduate degrees and experience beyond an associates degree, but community and technical colleges may find opportunities for related continuing education and perhaps future certifications in this area.

Specific Roles of Community and Technical Colleges

Overall, the growing need for people with a variety of Homeland Security knowledge, skills, and abilities (KSAs) will provide Texas community and technical colleges with many opportunities to fulfill their missions of contributing to the well being of the State and providing attractive employment opportunities for their graduates. In fact, the governance of Texas community and technical colleges by local entities ensures an understanding and responsiveness to local workforce needs. For example, colleges with existing relationships with employers that have a need to severely restrict access to their facilities (chemical refineries, airports, etc.) with biometrics technology should be responsive to modifying existing network security programs to include a biometrics track if an unmet demand for employees with these skills exists. Additionally, in many instances the State’s colleges provide valuable training for local first responders (e.g., emergency medical technicians (EMT), paramedics, fire fighters, police, etc.). Colleges can expand these training programs to include training and certification related specifically to homeland security tasks (e.g. nurse certification training in bioterror diseases like smallpox and anthrax) if needed.

Obviously, the experience, structure, and charge of the State’s community and technical colleges make them particularly well suited for training individuals needed to support these requirements. In some instances there will be a demand for graduates with Associate Degrees in Homeland Security, in other areas there will also be a need for continuing education training for a variety of people trained and employed in other, related areas such as nursing and construction technology. The programs being developed by the Homeland Security Curriculum Consortium and its associated colleges will provide a structure for training both of these groups. Although other colleges may have different training requirements, each college planning training in these areas will be well advised to become familiar with the HSCC programs.

Texas is home to some of the nation’s most critical infrastructure: international airports, international seaports, highways, border crossings, oil pipelines, chemical refineries, utilities, and much more. Protecting this infrastructure and the citizens of the State from harm is a huge task. As the American Association of Community College points out, the State’s community and technical colleges will need to create strategic long-term relationships with our state agencies and the U.S. Department of Homeland Security to keep their roles and resources at the forefront of the dialogue. Local, state, and national interests have an enormous investment in community and technical colleges. The failure to fully utilize these resources could have catastrophic consequences.
Appendix: Federal Government Programs

On October 1, 2003, President Bush signed into law the Department of Homeland Security’s $37.6 billion dollar Fiscal Year 2004 Budget. The following section contains excerpts from that budget, which detail how a significant portion of those monies were allocated.

Port Security

$125 million dollars has been allocated for port security grants that fund security planning and projects to improve dockside and perimeter security at the nation’s ports. The money will fund upgrades such as patrol boats in harbors, new command and control posts, communications tools for better intelligence gathering, and surveillance equipment at roads and bridges.

$64 million dollars has been allocated to support technology for non-intrusive inspection (NII). This will add to a variety of port inspection assets supported from prior year funding, including radiation detection systems, large scale x-ray machines for trucks and oceangoing shipping containers, mobile vehicle and cargo inspection systems (VACIS), and isotope identifiers for international mail and express courier hubs. The advantage to importers whose cargo warrants increased inspection will be more efficient, timely, and less costly inspections than the alternative of physical removal of cargo from conveyor belt systems.

$62 million dollars has been allocated for the Container Security Initiative (CSI) that deploy teams of inspectors, special agents, and intelligence analysts to 20 foreign “mega-ports” and approximately 10 other strategic ports to inspect containerized cargo for weapons of mass destruction before it is ever shipped to the United States.

Aviation Security

Of nearly $4.6 billion in Transportation Security Administration (TSA) funding, specific funding for programs in aviation security include:

- $150 million to purchase explosives detection systems; and
- $250 million to install these systems in airports.

Another $85 million is allocated to improve air cargo security, including:

- $30 million to enable TSA to improve its oversight of the known shipper program, using a risk-weighted freight screening system that will identify pieces of cargo that require closer scrutiny before being loaded on passenger aircraft. Funds will also enable TSA to hire an additional 100 staff to perform more in-depth audits of shipper compliance with the known shipper requirement; and
- $55 million to be used by TSA’s Research and Development to pursue a variety of technological solutions that would allow for the most efficient and targeted inspections of cargo transported on passenger aircraft.

Additionally, the Budget provides $60 million dollars for the research, development, testing and evaluation of an anti-missile device for commercial aircraft.

Information Analysis and Infrastructure Protection

A total of $839.3 million is provided for information analysis and infrastructure protection, including:

- $28 million for threat determination and assessment, which provides strategic assessments of our nation’s critical infrastructures and key assets, including 168,000
public water systems; 300,000 oil and natural gas production facilities; 4,000 offshore platforms; 278,000 miles of natural gas pipelines; 361 seaports; 104 nuclear power plants; 80,000 dams; and tens of thousands of other potentially critical targets;

- $84.2 million for infrastructure vulnerability and risk assessment, which will develop and maintain a complete, accurate, and prioritized mapping of the nation’s critical infrastructures and key assets including agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical and hazardous materials, postal and shipping, and monuments and icons;

- $345 million for remediation and protective actions, which includes work with state and local governments, and industry, to identify and prioritize protective measures; and to develop objective protection standards and performance measures; and

- $141 million for the National Communications System, which includes the emergency notification system, back-up dial-tone, government emergency telecommunications network, and wireless priority service.

Science and Technology

A total $918.2 million is provided for the Department of Homeland Security’s Science and Technology directorate, including:

- $127 million will be used to develop sensors and other countermeasures to prevent the illicit transport and use of radiological and nuclear materials within the United States;

- $70 million for the Homeland Security University Programs. This program will include the Homeland Security Scholars and Fellows program that will provide scholarships to undergraduate and graduate students pursuing scientific studies in homeland security;

- $39 million for developing a database of homeland-security related standards from private sector standards development organizations, for certification and accreditation models for products and services, for testing and evaluation protocols for commercial radiation detectors, and for developing standard chemical methods of analysis of high explosives, chemical warfare agents, and toxic industrial chemicals; and

- $38 million will be used to continue the deployment of the Urban Monitoring Program, also known as BioWatch. Through the BioWatch biosurveillance program, DHS, the Environmental Protection Agency and the Centers for Disease Control’s Laboratory Response Network provide early detection of bio-threats. These partners are working with state and local officials to implement an effective consequence management plan that incorporates the BioWatch system. In addition, these funds are also being applied to develop the next generation of bio-pathogen monitoring sensors.

Coast Guard (Port Patrols)

To protect America’s ports and waterways, the Coast Guard has made its largest commitment to port security since World War II, including over 35,000 port security patrols and 3,500 air patrols. Since 9/11, the Coast Guard has boarded over 2,500 vessels of interest, interdicted over 6,200 illegal immigrants, and created and maintained over 100 Maritime Security Zones.
Of $6.8 billion provided for the Coast Guard,

- $668 million is allocated to the Integrated Deepwater System Project, the Coast Guard’s multi-year recapitalization that will replace or modernize the Coast Guard’s large ships, aircraft, sensors, command and control systems, and logistics system. Deepwater funding in FY-04 including $143 million for aircraft, which will include the purchase of a CASA 235 maritime patrol aircraft; $303 million to be used in part for construction of the first 420-foot National Security Cutter; $101 million for use in part for continued development of a network-centric command and control system that will provide a common operating picture; $24.7 million for a common logistics information system; and continued development of the vertical unmanned aerial vehicle that will deploy from IDS cutters.

**Urban Security and Regional First Responders**

$4.037 billion is allocated to the Office for Domestic Preparedness for assistance to our nation’s first responders, including:

- $1.7 billion for formula-based grants to regional first responders. The emergency workers must spend those funds on equipment, training, planning and exercises related to preparing for terrorist events;
- $750 million for Firefighters Assistance Grants;
- $725 million for discretionary grants for high-threat, high-density urban areas; and
- $500 million for law enforcement terrorism prevention grants.

**President Bush’s Proposed Fiscal Year 2005 Budget**

President Bush’s proposed Fiscal Year 2005 Budget, which was released on February 2, 2004, provides $40.2 billion dollars for DHS programs, a $3.6 billion increase for the Department over the 2004 enacted level. Highlights of the 2005 Budget proposal, which still must be debated and approved by Congress, include:

- Over $890 million to support aviation security and other transportation security activities, including funds to improve integration of explosive detection system equipment into individual airports’ baggage processing to increase security effectiveness and promote greater efficiency;
- Nearly $450 million in new funding to maintain and enhance border security activities, including the expansion of the Container Security Initiative to pre-screen cargo containers in high-risk areas and improvements in DHS’ Detention and Removal Program; and
- $3.6 billion to support first-responder grants and assistance with better targeting to high-threat areas facing the greatest risk and vulnerability.
Terrorist Information Awareness Initiative

The Defense Department’s Defense Advanced Research Projects Agency (DARPA) has recently reorganized its Terrorist Information Awareness (TIA) Initiative, formerly known as the Total Information Awareness Initiative, to better address issues related to privacy. The original vision “behind the Initiative was to integrate public and private databases of all data relevant to monitoring the activities of potential terrorists and their supporters, and querying, analyzing, and mining the data.” The databases were to include such information as records of deposits and withdrawals from banks, money transfers through banks, enrollment in schools, records of entry into and departure from the US, records of travels via airlines and car rentals, purchase records for goods and services using credit cards, etc. However, the TIA was reorganized after several politicians and civil libertarian groups raised questions about the privacy implications of the program.

Terrorist Threat Integration Center

President Bush authorized creation of the Terrorist Threat Integration Center to integrate access to the databases of various federal agencies, including the Department of Homeland Security, CIA, FBI, INS (Naturalization and Immigration Services), etc. in order to identify terrorists and track their activities. The Center should allow analysts to query, analyze, and mine the central database to create a picture of terrorist activities in a much more efficient manner than has been possible in the past.

Transportation Workers Identification Center

The Transportation Workers Identification Card (TWIC) requires that all of the nation’s 15 million transportation workers, including truck drivers and airline stewardesses, carry an ID card that contains some form of biometric identification (fingerprint, most likely), a photograph, and biographical information.

Patriot Act

The Patriot Act requires federal agencies to record and track the movement of foreign citizens to and within the United States using technical means. A subsequent piece of legislation, called the Enhanced Border Security and Visa Reform Act, defines “technical means” as biometrics. The Act requires that all border crossings and airports have this technology installed by the end of 2004.

US VISIT and Immigrant Status Indicator Technology

In June of 2004, DHS awarded a $10 billion dollar contract for the US Visitor and Immigrant Status Indicator Technology (US VISIT) project to the Smart Border Alliance, led by prime contractor Accenture. Other companies in the Alliance include Austin based Dell Computers, Raytheon, SRA International, and the Titan Corporation. This system will provide the capability to record the entry and exit of non-US citizens into and out of the US, and provide officials with biometric information about persons who are in the US in violation of the terms of their admission to the US.

Bio-Terrorism Preparedness Act

In June of 2002, President Bush signed into law a bioterrorism bill that provided $4.6 billion dollars for improvements to U.S. bioterrorism defenses. In June of 2004, the Department of Homeland Security granted $498 million dollars to hospitals nationwide to improve their ability to respond to a biological attack. Over $33 million dollars of this grant went to hospitals located in Texas.

Joint Terrorism Task Forces

“To protect America from terrorist threats, the FBI has increased the number of counter-terrorism agents by nearly 40% and has expanded to 66 Joint Terrorism Task Forces nationwide. Through its new National Threats Warning System, the FBI has disseminated more than 50 warnings to over 60 Federal agencies and 18,000 state and local law enforcement agencies since 9/11.”137

Civilian Corps Councils

“To protect America’s neighborhoods, local Citizen Corps Councils have been formed in 51 states and territories, enlisting thousands of individual citizens to make their communities safer, stronger and better prepared. Community Emergency Response Team training has been conducted in 244 localities in 42 states. The President’s DHS Budget for 2004 provided $40 million for the Civilian Corps.”138

Dallas-Fort Worth Homeland Security Alliance

Formed in October 2002, the Dallas Fort Worth Homeland Security Alliance was created to address the vulnerabilities in homeland security in Dallas, Fort Worth (DFW) and throughout North Texas. The Alliance’s mission is to identify solutions and technologies that effectively address security and emergency preparedness required to respond to threats and attacks, and to address identified vulnerabilities in critical infrastructure segments. The DFW Homeland Security Alliance is comprised of representatives from the private and public sector to address the vulnerabilities within market segments in the Homeland Security arena. The group identifies solutions and technologies that will effectively address security and emergency preparedness, required to respond to threats and attacks.

Texas Seaports Grants

Texas seaports have won nearly $8.5 million dollars this year in anti-terror grants for projects such as risk assessments and command facilities. The money will help employ new security technologies. “For example, the Port of Houston – the nation’s largest in terms of foreign trade and second largest in tonnage – received $1.5 million for a new command and control center that local, state, and federal agencies can use to monitor emergencies ranging from hurricanes to terrorist attacks.”139 Eight other ports are using Transportation Security Administration grants for risk assessments, surveillance systems, lighting, command facilities, cameras, fencing, electronic detection equipment, and access control. They include: Port of Beaumont, Navigation District of Jefferson County ($560,000), Port of Corpus Christi ($560,000), Brazos River Harbor Navigation District, Freeport ($85,000), Port of Galveston ($1,611,206), Dynegy Midstream Services Houston ($60,000), LBC Houston LP, Houston ($142,000), BASF Corporation, New Orleans, Freeport ($220,000), Port of Texas City ($1,735,883). These grants were among 79 totaling $92.3 million awarded last summer for port security.

University Research Project

On July 9, 2003, The University of Texas at Austin announced it will receive $5 million from the State thanks to U.S. Sen. Kay Bailey Hutchison, R-Texas. With this funding, private sector businesses will work with the university to create a biological and chemical weapons detection program.

American Institute of Homeland Defense

The American Institute of Homeland Defense (AIHD) in San Antonio is offering courses for law enforcement personnel leading to a Certificate in Investigating, Preventing, and Surviving Terrorism.

University of Texas Biological and Chemical Countermeasures Program

The Biological and Chemical Countermeasures Program for the Institute for Advanced Technology University Affiliated Research Center at The University of Texas at Austin is developing resources that will counter biological/chemical threats and terrorism.

The Texas Center for Homeland Security Training

The Lamar Institute of Technology (LIT) in Beaumont, Texas has launched the Texas Center for Homeland Security Training. Through a partnership with AIHD, LIT will offer courses for first responders, emergency managers, and corporate security personnel. Five other colleges – St. Phillips College (San Antonio Community College District), Southwest Texas Junior College, Houston Community College, Texas State Technical College Waco and Texas State Technical College Harlingen, have signed Memorandums of Understanding with the Center, agreeing to jointly develop certified training and accredited education in the practical application of homeland security principles and practice.

Center for Infrastructure Assurance and Security

The Center for Infrastructure Assurance and Security coordinates efforts between the University of Texas at San Antonio, government agencies at the city, county, state, and federal levels, private information assurance and security (IAS) companies, 2-year and 4-year colleges, training institutions, and research institutions. The CIAS serves “as a source for funds and talent supporting basic and applied research to leverage San Antonio’s IAS strengths as part of the solution to the Nation’s Homeland Defense needs. The CIAS works closely with the world renowned “Security Hill” and its agencies, the Air Intelligence Agency [Lackland AFB], the Air Force Information Warfare Center, the Cryptologic Systems Group, and the Air Force Computer Emergency Response Team, to perform research and development on critical and complex security matters.”

Texas A&M University System

“The National Response and Rescue Training Center under the Texas A&M University System is a member of the National Domestic Preparedness Consortium, set to receive $80 million in funding for homeland security programs nationwide under the 2005 Homeland Security Appropriations Bill. As one of four consortium members, the training center will receive one quarter, or $20 million. The consortium is a partnership created in 1998 made up of Texas A&M University, Louisiana State University, New Mexico Institute of Mining and Technology, and the Departments of Homeland Security and Energy. It was created to provide a focused, threat responsive, long term national capability for emergency first responders.”

---

140 http://utsa.edu/cias/darkscreen.html
National Strategy to Secure Cyberspace. President Bush directed the development of the National Strategy to Secure Cyberspace to ensure that America had a clear roadmap to protect a part of its infrastructure so essential to the Nation’s way of life. The strategy was developed in close collaboration with key sectors of the economy that rely on cyberspace, State, and local governments, colleges and universities, and concerned organizations. The Strategy was released on February 14, 2003.

The National Strategy for Physical Protection of Critical Infrastructures and Key Assets outlines the strategic objectives that underpin the national infrastructure and key asset protection effort including: (a) identifying and assuring the protection of those infrastructure and assets the Nation deems most critical; (b) providing timely warning and assuring the protection of those infrastructures and assets that face a specific, imminent threat; and (c) assuring the protection of other infrastructures and assets that may become targets over time by pursuing specific initiatives and enabling a collaborative environment between the public and private sector. The Strategy was released on February 14, 2003.

President Bush’s 2004 Department of Homeland Security Budget provides a look at the spending priorities of the Department of Homeland Security. The budget includes a total of $37.6 billion, 11 percent more than the 2003 level and over 64 percent more than the FY 2002 level for these activities.

Guide for the Selection of Chemical and Biological Decontamination Equipment for Emergency First Responders. This publication by the National Institute of Justice provides information for emergency first responders about the selection and use of chemical and/or biological decontamination equipment for various applications.

The Office for Domestic Preparedness Training Strategy addresses the most basic of issues and questions confronting the preparation of our Nation’s first responders to respond to WMD incidents. These questions include: Who should be trained? What tasks should be the trained to perform? What training/instruction methods and training sites need to be pared with which tasks to maximize success in training? What methods are most capable of evaluating competency and performance upon completion of training; and What gaps need to be remedied in existing training to assure consistency with the findings of the training strategy?

Jane’s Facility Security Handbook was produced for the Division of Emergency Management, Texas Department of Public Safety, by Jane’s through a grant from the Federal Emergency Management Agency. The Handbook provides recommendations for first responders in planning for, preventing and responding to terrorist threats/attacks on a wide range of physical infrastructure including buildings, hospitals, educational institutions, transportation systems, utilities, entertainment facilities, and special events.

The Homeland Securities Industries Association (HSIA) Policy Forum Paper on Airport Security urges a comprehensive systemic approach to airport security. HSIA outlines a 3 stage general approach to airport security, that is applicable to other physical infrastructure: prevention, protection, and reaction.

Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response. This publication was prepared by an Institute of Medicine committee of medical experts on the effects of biological and chemical weapons. The Committee on R&D Needs for Improving Civilian Medical Response to Chemical and Biological Terrorism Incidents identifies the R&D efforts needed to implement recommendations in key areas: pre-incident intelligence, detection and identification of chemical and biological agents, protective clothing and equipment, early recognition that a population has been covertly exposed to a pathogen, mass casualty decontamination and triage, use of vaccines and pharmaceuticals, and the
psychological effects of terror. The book also addresses the differences between a biological and chemical attack, the distinct challenges to the military and civilian medical communities, and other broader issues.

The Practicality of Pulsed Fast Neutron Transmission Spectroscopy for Aviation Security. This publication by the National Material Advisory Board assessed the practicality of pulsed fast neutron transmission spectroscopy (PFNTS) for detecting explosives in passenger baggage and cargo in an airport. The report compares the capabilities of PFNTS with the capabilities of explosives-detection equipment currently available for deployment and with the expected future development of current equipment.

Everything You Need To Know About Biometrics. This white paper by Erik Bowman of Identix Corporation provides an excellent discussion of the advantages and disadvantages of different biometric technologies from an economic and public acceptance perspective.

Biometrics Measure Up Homeland Security. This article by Winn Hardin in the April 2003 edition of Homeland Security Solutions Magazine provides an excellent overview of the various biometric technologies. The article also discusses the biometric implications of various pieces of legislation passed in the wake of 9/11 including the Patriot Act, the Aviation and Transportation Security Act, and the Enhanced Border Security and Visa Reform Act.


Data Mining for Homeland Security by Jose Mena provides an overview of data mining tools that could be employed in the Homeland Security arena.

On US Homeland Security, Data Mining, and Civil Liberties by Won Kim provides an overview of the technical and civil liberties issues raised by DARPA’s Terrorist Information Awareness Initiative.

On Database Technology for US Homeland Security by Won Kim provides an overview of various database techniques that could be employed in the Homeland Security arena. Important issues covered in the paper include data mining, legacy databases, and federated databases.

Protecting Information The Role of Community Colleges in Cybersecurity Education is a report from a Workshop Sponsored by the National Science Foundation and the American Association of Community Colleges. The workshop involved over 90 experts in computer, network, and information security from community colleges, four-year institutions, business, industry, and government who convened to focus on how community college resources could be utilized and further developed to help educate a cybersecurity workforce.

Layered Network Security: A Best Practices Approach a white paper by Mitchell Ashley of StillSecure Corporation discusses, at a foundation level, the layered approach for securing information technology networks. The paper emphasizes that the layered approach is both a technical strategy, encompassing adequate technical measures that should be put in place at different levels within a network infrastructure, and an organizational strategy, requiring buy-in and participation from senior level management all the way down.
Appendix: Experts Interviewed

Steve Cooperman, Vice President, Oracle Homeland Security Solutions, for providing information about the Information Management challenges the government faces in ensuring Homeland Security.

Jim Wrightson, Vice President of Homeland Security, Lockheed-Martin, for providing information about the role of large scale system integrators (DoD contractors) in Department of Homeland Security port security, critical infrastructure and pattern analysis (data mining) initiatives.

Rex Richardson, Chief Scientist, SAIC Cargo Inspection Operation-San Diego, for providing information about the training requirements and employment opportunities for Cargo and Baggage Inspection Systems technicians.

Glen McNeil, Senior Director of Strategic Engineering, SAGEM Morpho, Inc., for providing information about federally mandated biometric initiatives and employment opportunities for technical and community college graduates in the biometrics area.

Lori Bush, Senior Adviser, Cisco Homeland Security Group, for providing information about security issues related to networking in government information technology domains.

Jesus Mena, CEO of Webminer and author of “Investigative Data Mining for Security and Criminal Detection,” for providing information about the use of data mining tools in Homeland Security applications.

Jack Colley, State Coordinator, Governor’s Division of Emergency Management-Department of Public Safety, for providing information about the role of DPS in State Homeland Security activities.

Retired Major General Todd Stewart, Director, Program for International and Homeland Security at Ohio State University and also Executive Director, National Academic Consortium for Homeland Security, for providing information on academic institutions (2 year and 4 year) offering Homeland Security programs.

M. Paul Collier, Executive Director, The Biometric Foundation, for providing background information on the use of biometrics in commercial, government, and military applications.

Dr. Melissa Stark, Assistant Director for Educational Programs, Purdue Center for Education and Research in Information Assurance and Security, for providing an overview of continuing education programs for the Center for Education and Research in Information Assurance and Security at Purdue University.

Dr. Walter McCollum, Biometrics Education Program Manager, Department of Defense Biometrics Management Office, for providing an overview of the Army’s Graduate Certificate Program in Information Assurance and Biometrics that will be offered through the College of Engineering and Mineral Resources at the University of West Virginia.

Gerald Adams, former Senior Advisor to Deputy Attorney General of Texas, Jay Kimbrough, for providing an overview of the Texas Department of Homeland Security and its interaction with 22 Council of Governments and Regional Councils.

Robert Weaver, Deputy Special Agent in Charge N.Y. Electronic Crimes Task Force, United States Secret Service, for providing an overview of the Secret Service’s approach to conducting vulnerability assessments and Homeland Security in the Information Assurance arena.
Dr. Robert Krienke, President, Lamar Institute of Technology, for his guidance and unwavering support in the development of the Texas Center for Homeland Security Training at the Institute.

Sam Williams, Vice President for Academic Affairs, Lamar Institute of Technology, for providing an overview of the activities of the Texas Homeland Security Consortia.

Jim Doane, Director of Homeland Security and Criminal Justice Training, Lamar Institute of Technology, for providing an overview of the Homeland Security curriculum at the Lamar Institute of Technology.

Mel Mireles, Director, Enterprise Operations Division, Texas Department of Information Resources, for providing an overview of his office’s role in Homeland Security and possible employment opportunities for residents of the State.
Program of Study: CS (Track 1)

Participants in the Computer Science Track of the Information Assurance Education Graduate Certificate Program (IAEGCP) will take 9 credit hours in computer science courses and 2 credit hours in curriculum and instruction courses; all courses are taught by information assurance experts. Because the program is condensed into an 8-week period, coursework will be intense. Participants will be expected to do independent reading for each class before the program begins. Participants who successfully complete the requirements of the program will receive a graduate certificate from the Department of Computer Science as well as a certificate from CERIAS.

Courses:

**CS 526 Information Security**
Basic notions of confidentiality, integrity, availability; authentication models; protection models; security kernels; secure programming; audit; intrusion detection and response; operational security issues; physical security issues; personnel security; policy formation and enforcement; access controls; information flow; legal and social issues; identification and authentication in local and distributed systems; classification and trust modeling; risk assessment.

**CS 555: Cryptography**
Concepts and principles of cryptography and data security. Cryptography (secret codes): principles of secrecy systems; classical cryptographic systems, including Vigenere and Vernam ciphers; the Data Encryption Standard (DES); public-key encryption; privacy-enhanced email; digital signatures. Proprietary software protection; information theory and number theory; complexity bounds on encryption; key escrow; traffic analysis; attacks against encryption; basic legal issues; e-commerce; and the role of protocols.

**CS 626: Advanced Information Assurance**
Advanced topics in information assurance, including selections from the following: penetration testing, formal verification of systems, formal models of information flow and protection, distributed system authentication, protocol design and attack, computer viruses and malware, intrusion and anomaly detection models, multi-level security, active defenses, investigation and forensics, network firewalls, anonymity and identity, e-commerce support, and database security models and mechanisms. Offered every third semester.

**EDCI 590 Design and Development of Instructional Materials and Resources**
Instructional skills development; instructional analysis; instructional strategies; producing implementing, and testing instructional materials, labs, case studies, and problems; formative and summative evaluation; curriculum development; and curriculum scope and sequence.
Purpose

The object of the Concepts in Biometric Systems and Information Assurance 5-Day Short Course is to present an introduction to the principles of operation, design, testing, and implementation of biometric systems and the legal, social, and ethical concerns associated with their use.

Course Description

In the Concepts in Biometric Systems and Information Assurance 5-Day Short Course, students are introduced to a variety of techniques used in identification and verification of individuals, the physiological basis of these techniques, and the algorithms and statistical methods employed to achieve acceptable false-accept and false-reject ratios. Major and emerging biometric technologies, testing and evaluation, standards, and case studies are discussed.

This Concepts in Biometric Systems and Information Assurance 5-Day Short Course is offered to all government personnel (military and civilian) and contractor personnel who meet the program acceptance requirements. The course is structured to provide an overview of the topics that comprise the Information Assurance and Biometrics Graduate Level Certificate Program and to meet the education needs of civilian and military personnel who have a requirement for biometric knowledge in order to perform their duties.

The Concepts in Biometric Systems and Information Assurance 5-Day Short Course is generally taught at West Virginia University (WVU). For groups of 10 or more participants, arrangements can be made to have the WVU Mobile Training Team present the course at off-campus locations throughout the U.S. See the Contact Information section of this brochure for more Information on making these arrangements.

Course Content

The following content is covered in the Concepts in Biometric Systems and Information Assurance 5-Day Short Course:

Part 1: Biometric Systems
- Definitions, Terminology, and History
- Technological, Ethical, and Socio-legal Implications
- System Architecture, Subsystems and Components
- Signal/Image Processing, Pattern Recognition
- Classification and Templates
- Matching Algorithms
Part 2: Performance (Test and Evaluation)
False Accept Rate (FAR)
False Reject Rate (FRR)
Best Practices Document
Volunteer Crew and Representativeness
Issues in Estimation of FAR and FRR
Issues in Required Operational Capability (ROC) Estimation
Introduction to Statistical Biases

Part 3: Information Assurance
Identification and Authentication
Overview Principles of Cryptography
Origins
Basic Principles of Modern Cryptography
Introduction to Security protocols
Legal and Ethical Issues in Computer Security
Homeland Security: A Technology Forecast
Implications for Community & Technical Colleges in the State of Texas

The events of September 11, 2001 brought immediate attention to the challenges of internal security in the United States. The realization of these challenges resulted in a number of actions by federal, state, and local governments, including the establishment of the Department of Homeland Security (DHS). This report presents information, ideas, and concepts designed to assist Texas community and technical college leaders in making reasoned decisions about the design, initiation, and conduct of HS programs at their institutions. The report includes analyses of seven technology areas that provide the technical underpinnings for the nation's homeland security agenda. These areas include:

- Identification specialists
- Network security specialists
- Weapons of mass destruction (WMD) detection specialists
- WMD mitigation and decontamination specialists
- Concealed explosives specialists
- Critical infrastructure security specialists
- Pattern analysis specialists

This research was conducted by the Technology Futures Inc. and Texas State Technical College System from late 2003 to early 2004.

Programs for Emerging Technologies
In 1999, the Texas State Senate mandated Texas State Technical College System Operations to “develop and administer a program to forecast the types of technical education programs that are needed to maintain and improve the State’s economic and technical competitiveness.” (SB1819) In 2001, the Texas Higher Education Coordinating Board provided funding under a Carl D. Perkins grant to Texas State Technical College System (TSTC) to develop a program, later called the Program for Emerging Technologies, for accomplishing the Senate's goals with regard to the state's community and technical colleges. Programs for Emerging Technologies (PET) identifies and forecasts new and emerging technologies and respective future curriculum development opportunities for Texas community and technical colleges.

For additional information contact:
Michael A. Bettersworth
Associate Vice Chancellor for Technology Advancement
Texas State Technical College System Operations
3801 Campus Drive, Waco, Texas 76705, U.S.A.
michael.bettersworth@tstc.edu 254.867.3995

Funded by the Carl D. Perkins Vocational and Technical Education Act of 1998 as administered by the Texas Higher Education Coordinating Board.

www.forecasting.tstc.edu