FEBRUARY 2004 / VOLUME 2, NUMBER 8

THE CIP REPORT

Healthcare Sector

Call to Action 2
Legal Insights: Organizing to Protect the Sector 4
INOVA: Preparedness 5
Protecting the Nation's Blood Supply: Research Update . .6
HSPD-9 6
Healthcare Sector Coordinating Committee 7
USFA Announcement 7
Elevating Bioterrorism Preparedness in Hospitals .9
Protected Critical Infrastructure Information Program 11

CIP Project Staff

John McCarthy, *Executive Director*

Emily Frye, *Associate Director, Law and Economics Programs*

Kevin "Kip" Thomas, *Associate Director, Research Programs / Research Associate Professor*

Dr. John Noftsinger, *Executive Director, JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Project Liaison*

Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click here.

With an increased focus on biological terrorism, the nation is intensifying its focus on the need for reliable healthcare and the provision of vital human services. As with the nation's other critical infrastructures, the sector is experiencing a dramatic rise in cyber and physical threats. The risk of terrorist acts and escalating world events intensify growing security concerns for the protection of health information, physical structures, and key assets.

The Healthcare Sector supports the essential delivery of patient care services through its facilities, systems, technologies, and related functions. The goods and services it provides contribute to a strong economy, public safety, and confidence.

The Healthcare Sector is highly sophisticated, complex, and increasingly vulnerable, as the sector relies heavily on human capital as well as cyber and physical components. Human capital encompasses prevention, surveillance, laboratory services, and personal heath services. The sector's cyber infrastructures support information technology equipment and systems, which house and transmit patient care information. Physical infrastructures support the access and functionality of health and medical facilities essential to providing patient care services, such as hospital facilities, blood supply, vaccines, medicines, and equipment.

THE TECH CENTER
National Center for Technology & Law
CRITICAL INFRASTRUCTURE PROTECTION PROJECT

Healthcare is rapidly becoming more interconnected as suppliers, payers, providers, and patients are reaching new levels of information exchange. The healthcare industry is poised to achieve new levels of quality, safety, and efficiency through the adoption of information technology, but must remain aware of the associated risks and necessary precautions.

This month's CIP Report is focused on the Healthcare Sector. This issue introduces readers to the work of the Healthcare Sector Coordinating Council, the Healthcare ISAC, and other research and related initiatives.

Excerpt from

Securing the Healthcare Sector: A Call to Action

A Growing Need for Action

The terrorist events of September 11, 2001, demonstrate with shocking clarity the United States' increasing vulnerability to terrorist attacks. The Attorney General's report from 1997 states that our country is becoming more and more dependent on computer-controlled critical functions conducted within networks that remain largely unsecured. As a result, the President has asked the Homeland Security Council and the Department of Homeland Security to work with each critical sector of the economy to ensure delivery of those goods and services. The Department of Homeland Security was created by the Homeland Security Act of 2002, and the Homeland Security Council is a coordinating body similar to the National Security Council. These actions demonstrate the increasing level of federal efforts to protect the American people against attacks to their critical infrastructures.

Building an Industry Response

In his 2002 National Strategy for Homeland Security, the President identified 13 critical infrastructure sectors: agriculture, food, water, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical and hazardous materials, postal and shipping, and public health. The USA Patriot Act defines critical infrastructures as "systems and assets, whether physical or virtual,

so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

America's critical infrastructure sectors provide the foundation for our national security, governance, economic vitality, and way of life. Furthermore, their continued reliability, robustness, and resiliency create a sense of confidence and form an important part of our national identity and purpose. Critical infrastructures frame our daily lives and enable us to enjoy one of the highest overall standards of living in the world.

The facilities, systems, and functions that comprise our critical infrastructures are highly sophisticated and complex. They include human assets and physical and cyber systems that work together in processes that are highly interdependent. They also consist of key nodes that, in turn, are essential to the operation of the critical infrastructures in which they function.

Critical infrastructure sectors such as agriculture, food, and water, along with public health and emergency services, provide the essential goods and services that Americans depend on to survive.

Energy, transportation, banking and financial services, chemical manufacturing, postal services, and shipping sustain the Nation's economy and make possible and available a continuous array of goods and services.

The healthcare sector, as it becomes increasingly interconnected, grows more vulnerable to physical attack and cyber and information warfare. To mitigate these growing risks, the industry must develop an effective preparedness, awareness and response strategy for protecting the Nation's ability to deliver medical services. Developing this strategy poses a number of substantial challenges. Ultimately, the success of *(Continued, Page 3)*

Call to Action *(Cont. from Page 2)*
protecting and strengthening the security of the healthcare industry depends on a voluntary partnership between the private sector and federal, state, and local governments.

A security model for the healthcare industry will be an integral part of the national planning process led by the new Department of Homeland Security (DHS). Already, our industry has participated in the creation of the National Strategy to Secure Cyberspace, released by the White House in February 2003. As one of the critical infrastructure sectors, we continue to evaluate our current state of technology by examining cyber security threats and vulnerabilities. To mitigate current and future vulnerabilities introduced to the healthcare industry infrastructure through technology, we must develop a sector alert and response strategy for cyber and physical threats. The collaboration of various industry players is key to alerting and protecting sector organizations and responding to the growing cyber and physical security threats facing healthcare. Protecting the Nation's healthcare delivery system depends on three factors:

1. An improved understanding and awareness of the current healthcare state by industry players;

2. The industry's commitment to partaking in cyber and physical security initiatives; and

3. The industry's focus on protecting cyber and physical infrastructures essential to the delivery of patient care.

The following sections discuss these factors further.

Current Healthcare State

Primarily, discussions regarding the current state of healthcare take into account three key elements: the population that the industry serves; the infrastructure, which includes physical facilities and technologies associated with the delivery of care; and the industry's financing, composed of both private and government healthcare coverage for consumers. Together, these elements drive the future state of affairs regarding security for the healthcare sector as a whole.

Population:

The term "population dynamics" refers to a population's demographics and projected growth.

It is estimated that the U.S. population will increase 20 percent by 2020. Meanwhile, the population also continues to age. The current projection indicates 20 percent of the population will be over 65 by 2025[1]. Other factors affecting population dynamics are ethnic mix, incidence of disease, culture, and lifestyle-all of which are directly associated with the overall health of the population. These population factors directly affect the type of care consumers receive, their access to care, and the financing of the care provided. As a result, the private sector and the government continually evaluate the demand of healthcare services in order to provide appropriate care to consumers.

Recent trends in patient healthcare decisions reflect an apparent increase in consumer empowerment. The healthcare industry's continued cost shifting to patients has caused individuals to take on greater responsibilities with respect to the healthcare products and services they receive, thereby greatly accelerating consumerism. As a result, concerns related to access and convenience of medical care will require the healthcare industry to respond in a manner similar to that of other service industries by empowering patients to manage their overall healthcare experience. More and more, patients are managing their health and the health of their family members online. Research has shown increasing patient use of the Internet to research medical conditions, communicate with physicians and caregivers, and access clinical records. A national survey conducted by Pew Internet and American Life (2002) found that 62 percent of Internet users, or 73 million people in the U.S., have gone online in search of health information[2].

Infrastructure:

Several drivers, including technology, obsolescence, capital costs, and workforce availability, shape the healthcare infrastructure. The consistent introduction of new
(Continued, Page 17)

LEGAL INSIGHTS

by Emily Frye

Organizing to Protect the Healthcare Infrastructure

by Guest Columnists
Tim Gladura, Vice President and Chief Security Officer, Cardinal Health Systems
Tim Zoph, Vice President and Chief Information Officer, Northwestern Memorial Hospital

The notion of shared critical infrastructure in the private sector seems to have taken root in a number of industries. In health and medicine, things have moved more slowly. This should hardly be a surprise, as this sector is one of the largest and most diverse enterprises in the U.S. economy. While there are a number of important companies with nationwide and often world-wide scope, caregiver to patient interaction is very much a local affair. There are tens of thousands of hospitals, clinics and community practices and just as many solo or small practices. Unlike other sectors such as energy, utilities or financial services, healthcare is in many ways a trillion dollar cottage industry.

Although the healthcare industry is difficult to precisely define due to its size and complexity, it is extremely important. Our sector has a myriad of physical and information assets that must work together across the nation and the world, yet it must also respond effectively to crises in local communities. We are part of and depend on the network of first responders, public health officials and government, and our links to ground transport, utilities and energy are pervasive. Disruptions of our critical infrastructure, either in a local environment or at the national and international level, are bound to have significant economic, social and human costs.

Healthcare was the last of the critical sectors identified by Presidential Decision Directive 63 to self-organize as a Sector Coordinator. While there had been a number of isolated efforts over the years to pull together a coordinating committee, it wasn't until a number of healthcare officials/leaders from industry and government were invited to the White House in the summer of 2002, that support began to solidify. The possibility of an Information Sharing and Analysis Center in healthcare and a need for the private sector to lead in information sharing was raised. A series of meetings was then held with representation from public health, government healthcare providers, pharmaceuticals, medical devices, services, payors and hospitals.

Unlike other sectors such as energy, utilities or financial services, healthcare is in many ways a trillion dollar cottage industry.

It was clear from the beginning that the sector needed a focus, and attendees at the meetings of late 2002 and early 2003 agreed, upon some discussion and a little controversy, to focus on patient care, both up stream and down stream, especially as provided in the private sector. A committee was established and formal linkages were made with colleagues in related government areas. The committee began to identify participants, looking to industry leaders, principally in information technology and security-related positions.

One of the early challenges was helping people understand that the term "public health" (as the sector was termed in PDD-63) has a specific and narrow meaning among health professionals. The term generally refers to the study of overarching health and disease issues, including such *(Continued, Page 5)*

Inova Health System: Disaster Preparedness Efforts

As the premier provider of healthcare services in the Northern Virginia area, Inova Health System is in a unique position to provide leadership in the design, implementation, and study of issues related to healthcare delivery as a result of conventional or unconventional terrorist acts or those resultant from large-scale disease outbreak events. Following the disastrous events of September 11, 2001, the bioterror attacks of October 2001, the sniper attacks of October 2002, and the most recent disaster related to Hurricane Isabel, there is ample evidence of increased need to better coordinate the acute healthcare delivery sector into the broad spectrum of emergency response entities, including the public safety, public health and emergency management communities. Long before the horrors of 9-11, Inova Health System has provided key leadership in disaster planning and response within the National Capital Region, the Commonwealth of Virginia, and for the nation.

Dan Hanfling, MD, chair of Inova Health's disaster preparedness committee

In the event of another terrorist attack in the National Capitol Region, Inova Health System will be a major participant in the *(Continued, Page 10)*

Legal Insights *(Cont. from Page 4)* things as tracking the numbers of people who contract a certain disease, determining the components of influenza vaccines and establishing response procedures for major epidemics. "Public health," which is carried on principally by government entities like the Centers for Disease Control (CDC) and local health authorities, is therefore quite different from the delivery of healthcare, the domain of public and private practices, as well as vendors and suppliers. It is not to denigrate the vital role that public health plays in these areas to observe that healthcare delivery is larger by several orders of magnitude and astonishingly complex. Sector coordination has thus focused on reaching this broader array of large and small, for-profit and not-for-profit, community and international based organizations, each engaged in a unique set of functions or services.

Once having clarified its mission in a collaborative "Call to Action," the organizing committee transformed into the Healthcare Sector Coordinating Council (HSCC). Secretary Thompson of the Department of Health and Human Services (HHS) formally recognized the Council as the Sector Coordinator for critical infrastructure protection within the healthcare industry in September 2003. The Council is now completing a strategic plan for its activities. We are building upon the experience of our colleagues in other sectors and the guidance of our sector liaison, HHS, and the Department of Homeland Security (DHS).

The challenges are manifold and raise significant questions. How can our sector reflect both an international agenda and the essentially local flavor of much of the industry? How do we meet the needs of large pharmaceutical or device companies on one end of the service spectrum as well as community physician practices on the other end? What are the overlaps of our physical and cyber infrastructures, and how do we address each? Should issues surrounding HIPAA security or other pressing business demands be incorporated into the HSCC services? The questions are many, as are the demands on professionals in our field. The HSCC and our many friends and colleagues in the field are committed to forming a partnership with Health and Human Services and the Department of Homeland Security to address these fundamental infrastructure concerns, and there is much to be done. Despite our late start, we would hope for some future commentator to remark on how well healthcare has taken to infrastructure protection and how much progress has been made in collaborative security. ❖

Protecting the Nation's Blood Supply Project Update

Karen N. Plante, FACHE
Arnauld Nicogossian, M.D.


Dr. Nicogossian

This research activity focused on epidemiological, biomedical, and technological aspects of blood supply protection. The team conducted an in-depth evaluation of the strengths and vulnerabilities of the existing processes and procedures in protecting the nation's blood products and blood supply infrastructure, and examined the policy issues related to enhancing their safety and security.

At the present time, as the project nears completion, the research team has completed the last of three workshops, and the final report is being edited. The following abstract summarizes some of the issues and findings; it was submitted for presentation to "Science and Technology in Context 2004", an interdisciplinary graduate student conference sponsored by the National Science Foundation.

Protecting the Nation's Blood Supply: Vulnerabilities and Policy Options

In the United States, blood and blood products are used every day to sustain patient health and well-being, support complex surgical procedures, and to serve as replacement cells for those suffering from inherited metabolic disorders or undergoing cancer therapy. Preservation of an adequate and safe blood supply is a critical aspect of the medical infrastructure. A real or perceived bioterrorist attack can theoretically disrupt the availability of blood products and undermine the confidence of the medical system within the general population. The blood collection, processing and distribution system in the United States is among the most controlled and protected components of our health care system. Due to the decentralized nature of the blood collection process and the maintenance of the unit-integrity of the blood (and blood components) collected, the blood supply could be considered more susceptible to direct contamination through unintentional human error than intentional efforts by would-be terrorists. Our research identified three vulnerabilities in the nation's blood supply system that have the greatest potential for compromise through terrorism. The aspects that are most vulnerable to terrorist attack are events that lead to a mass deferment of the donor pool, a compromise of public confidence in the safety of the system, and disruption of the distribution network. This research assesses these vulnerabilities, the implications that a compromise in one of these areas would have on the preservation of a viable blood infrastructure, and the policy implications for collection, processing and distribution of blood and blood products. ❖

NEW DIRECTIVE AIMED AT PROTECTING NATION'S FOOD SUPPLY

The Bush Administration has issued a decision directive to protect the nation's food supply from terrorist attacks, natural disasters, and other incidents. The Administration policy, issued as Homeland Security Presidential Directive 9 (HSPD-9), *Defense of United States Agriculture and Food* (January 30, 2004) directs government agencies to create security strategies to govern the U.S. food, manufacturing, and agriculture sectors.

HSPD-9 outlines specific activities Federal departments and agencies must undertake to protect agriculture and food economies. Requirements include performing vulnerability assessments, crafting mitigation strategies, planning for response and recovery, establishing education programs, researching new technologies, and increasing awareness and warning capabilities. Consistent with earlier policies, HSPD-9 places the Department of Homeland Security (DHS) in charge of coordinating all Federal efforts to protect the nation's critical infrastructure. However, HSPD-9 also orders the US Department of Agriculture (USDA), Health and Human Services (HHS), and the Environmental Protection Agency (EPA) to implement specific measures based on existing agency relationships and legal responsibilities.

USFA Announces Name Change For Its Critical Infrastructure Protection Information Center

New Name to Reflect Contributions to the System of Information Sharing and Analysis Centers

The United States Fire Administration (USFA) recently announced a name change for its Critical Infrastructure Protection Information Center. The new name, Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC), more accurately reflects the mission and responsibilities of its critical infrastructure protection officials and conforms to the system of ISACs supported by Homeland Security Presidential Directive-7. The EMR-ISAC is located at the National Emergency Training Center in Emmitsburg, MD.

The Critical Infrastructure Protection Information Center has performed the work of an ISAC for the emergency management and response sector since it began in October 1, 2000, in response to Presidential Decision Directive-63. Now, as the EMR-ISAC, it will continue to benefit emergency managers, firefighters, and emergency medical personnel through daily research on current CIP issues; receiving and processing threat intelligence; preparing and distributing weekly INFOGRAMs and periodic CIP Bulletins; forwarding Sensitive CIP Information to sector key leaders; developing instructional materials; and providing technical assistance to sector members.

HSCC

Healthcare Sector Coordinating Committee: Raising the Bar in Sector Cyber Security

The U.S. healthcare industry faces many security challenges and threats associated with protecting cyber and physical infrastructures. The industry has often lagged behind other critical service sectors, primarily with respect to IT and security investments. The sector now has the opportunity to assume a leadership role in cyber and physical security and begin with the end in mind. Now is the time when the industry's players can identify the threats and vulnerabilities facing healthcare infrastructures and-together with the government-collectively organize their efforts to eliminate or mitigate those risks to protect the delivery of healthcare, a critical part of the U.S. economy.

The healthcare sector requires a framework through which it can protect the industry from cyber and physical infrastructure threats. Industry collaboration, the adoption of best practices, the development of security standards, and the establishment of a governance structure for the inclusion of new IT systems, communication networks and physical networks are vital for the industry's future viability. The Healthcare Sector Coordinating Council (HSCC), a collaboration of leaders from across the diverse health and medical sector, is working to build such a framework to achieve fundamental and vital cyber and physical security objectives for the industry.

The charter of the HSCC is to protect the components of the healthcare industry's cyber and physical infrastructure that are essential to patient care delivery. The operational mission of efforts is to gather, analyze, and disseminate to its members an integrated view of the healthcare industry's cyber and physical threats and vulnerabilities in partnership with our national homeland security activities.

The HSCC is evaluating a number of models of information sharing and learning from the experience of colleagues in private and public sector ISAC's. The goal is to provide an opportunity for organizations in the healthcare sector to share information regarding threat, vulnerability, risk and controls and countermeasures. The expectation is that such information will come from a number of sources, the U.S. government and law enforcement agencies, technology providers and security associations, and from the private healthcare sector as a whole. Information is likely to be used for alerts and to develop awareness and response based on the state of the healthcare infrastructures and the national threat environment. Through the organization of the healthcare sector, information, such as industry best practices, may be shared among members and exchanged with the government through the Department of Homeland Security and

(Continued, Page 8)

HSCC *(Cont. from Page 7)*
Department of Health and Human Services. Most importantly, organization of the sector is being established on the principles of trust, commitment, respect and partnership to advance cyber and physical security for the industry, while increasing public trust and confidence in healthcare.

The healthcare infrastructure supports the essential delivery of patient care services. Healthcare facilities, systems, technologies, and functions comprise the critical healthcare infrastructure making it highly sophisticated, complex, and increasingly vulnerable. The healthcare industry is facing an increasing number of threats and vulnerabilities primarily to its cyber and physical infrastructure. HSCC is principally concerned with protection and response to cyber and physical attacks, yet it is critical to establish robust relationships with those entities addressing emergency preparedness threats, such as bioterrorism, or nuclear and chemical attacks.

There are underlying assumptions about the value of sector-wide information sharing. Its success in healthcare hinges on its ability to assure operational reliability, availability, and integrity. The information sharing network envisioned by HSCC is to be interconnected throughout the industry, making it key to national infrastructure operations. The quickly evolving nature of the current threat environment and the potential consequences the threats carry necessitate a faster, more efficient dissemination of information than ever before.

Meaningful participation across the healthcare sector should yield a number of benefits across the sector, and there are several operational programs to be pursued:

- **Industry-Wide Critical Information Sharing Model:** Healthcare organizations may receive and share appropriate vulnerability and threat information from within the industry, but will also exchange information with the Department of Health and Human Services as well as the Information Analysis and Infrastructure Protection directorate of the Department of Homeland Security.
- **Industry Alert Systems:** Organizations may receive industry vulnerability and threat alerts and early warnings of impending attacks, possibly through a secure web portal (Internet accessible with secure login) and email/pagers.
- **Industry-Specific Response Plan:** Response plans consistent with the National Response Plan are useful.
- **Cyber and Physical Security 'Best Practices':** These can be drawn from healthcare and other industries.
- **Industry-Government Relationship:** As many healthcare organizations are intertwined with government functions at the federal, state and local level, strong partnerships with government agencies will benefit all stakeholders.
- **'Raising the Bar' in Healthcare Cyber Security:** HSCC believes it is critical to plan, implement and evaluate improved security in the healthcare sector. Information sharing is a fundamental component of this mission. ❖

After 9-11: Elevating Bioterrorism Preparedness in Hospitals

Jenifer K. Murphy

James Madison University, Health Services Administration Program

Executive Summary

Following the terrorist attacks of September 11, 2001, bioterrorism preparedness became a high priority in hospitals. However, despite significant advancements in preparedness, many hospitals are still unprepared to deal with the impact of bioterrorism. The federal government has provided initial funding to state and local governments for bioterrorism preparedness, however much of this money has yet to reach hospitals. Efforts by hospitals to elevate bioterrorism preparedness should focus on several key areas. These are community involvement, educating hospital staff, improving information technology and disease surveillance, and acquiring additional equipment and staff. Hospitals should also make bioterrorism preparedness planning a regional effort.

Introduction

A war exercise conducted in 2001, before the September 11 attacks, simulated the release of smallpox. Within a thirteen-day period, the virus had infected thousands of people and spread across twenty-five states and into fifteen countries (McCarthy 2001). Subsequent to the terrorist attacks of September 11, hospitals in the U.S. had to cope with the threat of anthrax, SARS, and Monkey pox, and emergency preparedness became a high priority focus. Since that time, many hospitals made significant strides in their emergency preparedness (McCarthy 2001), but recently the sense of urgency of preparedness in hospitals appears to have declined somewhat. This is largely due to the perceived belief that an attack is unlikely to occur (Bartlett 2001). As centers of health and medical resources for their communities, hospitals need to remember that even if their locality is not a direct victim of an attack they will still be called upon for regional support and may have to treat victims. Bioterrorism has no boundaries and can happen anywhere and at anytime (Tieman 2002). All hospitals, not just those in high threat areas, should be prepared to combat the catastrophic and widespread effects of a bioterrorism. This paper addresses the need for hospitals to evaluate their current levels of bioterrorism preparedness and take the necessary actions and precautions to protect their staff, patients and the surrounding communities in the event of an attack. The federal government has provided some initial funding to prepare hospitals, but it is not enough to adequately to be adequately prepared. There are several aspects of bioterrorist preparation that hospitals should have in focus. These priority focus areas are promoting community involvement and communication, educating hospital staff and area primary care physicians, improving information technology, and acquiring additional equipment and staff to deal with a bioterrorist attack. An attack is seemingly inevitable and all hospitals, regardless of location and size, will feel the effects of bioterrorism.

Biological Agents and Current Hospital Preparedness Levels

There are other forms of terrorism *(Continued, Page 11)*

Jenifer K. Murphy placed first in the Hill-Rom Management Essay Competition, Undergraduate Division, sponsored by the American College of Healthcare Executives, for her essay entitled: "After 9-11: Elevating Bioterrorism Preparedness in Hospitals." Jenifer is a senior Health Services Administration major at James Madison University (JMU) who is from Virginia Beach, Virginia. She also serves as the President of the Student Chapter of the American College of Healthcare Executives at JMU. Jenifer plans on working in either hospital administration or ambulatory care when she graduates from JMU in May 2004, and eventually she will complete graduate study in Health Services Administration.

INOVA *(Cont. from Page 5)*
response efforts to such attacks. Inova Health System is has 5 acute care hospitals in northern Virginia, with 3 additional 24/7 free-standing emergency departments that will all be critical elements in the management of patients injured as result of terror attacks. Our facilities are equipped to manage chemical and radiological decontamination, with fixed decontamination showers that will provide for the decontamination of over 500 victims of exposure per hour across all of our facilities. Inova Health System has also mobilized a team of physicians and nurses vaccinated against the smallpox virus, who constitute a smallpox response team in the event of suspected smallpox cases arriving at any one of our facilities.

These efforts at increased preparedness have been relentless precisely because of our location in the Northern Virginia area. Our proximity to the CIA, Dulles Airport, National Airport, the Pentagon, high tech companies (AOL and others), and other national resources make it highly likely that Northern Virginia will be the target of future terrorist activity.

Inova's current contributions include:

- Providing centralized planning for a fully integrated, multi-disciplinary all-hazards disaster readiness approach undertaken by the Inova Health System, and as a part of the healthcare planning efforts throughout the Northern Virginia and National Capitol Region.

At this point in our history, support for health care institutions must be viewed in the same context as other national security imperatives, especially in the capital region. Hospitals must be recognized as part of the country's critical infrastructure and supported for the public safety efforts now expected of them.

--Dan Hanfling, Director of Emergency Management and Disaster Medicine for Inova Health System

- Providing leadership to the Commonwealth of Virginia and to the National Capital Region by facilitating the coordination of the health and medical operational response to disaster events, in cooperation with the Virginia Department of Health and the Department of Homeland Security, National Capital Region Coordinator by managing the MEDCOMM communications clearinghouse radio network.
- Providing leadership to the Commonwealth of Virginia and to the National Capital Region by specifically promoting the coordination of public health, public safety and emergency management cross-jurisdictional preparedness efforts.
- Providing leadership to federal efforts in disaster planning, specifically with the Department of Health and Human Services (including the Agency for Healthcare Research and Quality and the Centers for Disease Control), the Department of Homeland Security (including the Office of Domestic Preparedness, the Metropolitan Medical Response System, and the Federal Emergency Management Agency), and the Department of Defense.
- Promoting research and peer reviewed publications in the field of disaster medicine and emergency management.
- Providing legislative liaison to appropriate local, state, and federal legislators and agencies, including Congress.
- Providing subject matter expertise in order to shape legislative agendas to national organizations including the American Medical Association and the American Hospitals Association. ❖

DHS Launches Protected Critical Infrastructure Information Program to Enhance Homeland Security, Facilitate Information Sharing

The U.S. Department of Homeland Security recently announced the launch of the Protected Critical Infrastructure Information (PCII) Program. The PCII Program enables the private sector to voluntarily submit infrastructure information to the Federal government to assist the Nation in reducing its vulnerability to terrorist attacks.

Critical infrastructure includes the assets and systems that, if disrupted, would threaten our national security, public health and safety, economy, and way of life. Although these industries, services and systems may be found in both the public and private sectors, the Department of Homeland Security estimates that more than 85 percent falls within the private sector.

Under provisions of the Critical Infrastructure Information Act of 2002 (CII Act), information that is voluntarily submitted per those provisions will be protected from public disclosure until and unless a determination is made by the PCII Program Office that the information does not meet the requirements for PCII. If validated as PCII, the information will remain exempt from public disclosure. The rule establishing the procedures for PCII was published this week in the Federal Register. The PCII Program Office is part of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Directorate and is charged with receiving submissions, determining if the information qualifies for protection and, if validated, sharing it with authorized entities for use as specified in the CII Act.

Initially, the PCII Program Office will limit the sharing of PCII to IAIP analysts. PCII may be used for many purposes, focusing primarily on analyzing and securing critical infrastructure and protected systems, risk and vulnerabilities assessments, and assisting with recovery as appropriate. The IAIP Directorate plays a critical role in securing the homeland by identifying and assessing threats and mapping those threats against vulnerabilities such as critical infrastructure.

Effective immediately, members of the public who wish to submit information may do so through the PCII Program Office.

For more information about the PCII Program, or to access the PCII regulation, please visit the PCII Program Office website on *www.DHS.gov/pcii.* ❖

Bioterrorism Preparedness *(Cont. from Page 9)* and weapons of mass destruction the United States is certainly susceptible to and that hospitals also need to be prepared to handle. Some of these include chemical agents, power outages, radiation, and nuclear weapons. For the purposes of this paper, biological agents are felt to be of the greatest concern to hospitals because of the far-reaching effect a bioterrorist attack would have. The Centers for Disease Control currently list six diseases as Category A biological threats. Category A biological agents are those the "U.S. public health system and primary healthcare providers must be prepared to address" (Centers for Disease Control 2003). They are considered threats to national security, are highly transmittable, and have high mortality rates (CDC 2003). These agents are anthrax, botulism, smallpox, tularemia, viral hemorrhagic fever (VHF), and plague. Are hospitals adequately prepared to deal with the effects of these diseases? A study of 30 FEMA Region III hospitals completed in 2001 showed a majority of staff felt unprepared to deal with the mass casualties associated with a bioterrorist attack (Treat et al. 2001). None of the hospitals surveyed felt prepared for a bioterrorism attack, 73% only have a single decontamination unit, and 87% said they could only handle from 10-50 patients at a time (Treat et al. 2001). A 2003 study conducted by the American Hospital Association *(Continued, Page 12)*

Bioterrorism Preparedness *(Cont. from Page 11)* (AHA) shows hospitals are lacking in appropriate medical equipment to deal with mass casualties from bioterrorism. Furthermore, four out of five hospitals in the study did have plans in place to deal with an attack, but did not have policies for involving outside organizations, such as laboratories (Crosse 2003). Much of this lack of preparedness is due to hospitals operating individually and not coordinating their planning efforts with outside organizations (Barbera and Macintyre 2002). The AHA study makes several suggestions to hospitals for improving bioterrorism preparedness. Hospitals need to first develop policies to include local and state health departments in their bioterrorism response scenarios, and test these policies in JCAHO required drills. Staff education, especially in the emergency room, needs to be improved as well. There should also be an increase in critical medical equipment, such as ventilators, decontamination equipment, I.V. infusion pumps, hyperbaric chambers, and external pacemakers (Greene 2002).

What Should Hospitals Do?

It is difficult to prepare for the unknown. The unpredictability of bioterrorism makes planning for it extremely challenging because no one knows when an attack could actually occur. Bioterrorism preparedness plans are also extremely expensive to implement and maintain. Though the importance of bioterrorism preparedness cannot be argued, it is difficult for hospitals to spend money on equipment and systems that may never be used, especially in areas where the threat of an attack is low. While important progress has been made in hospital preparedness levels (McCarthy 2001), there are four main actions hospitals should take to increase their level of bioterrorism preparedness.

Community Involvement

Hospital bioterrorism preparedness needs to be a broad-based community effort coordinated by the hospital. In the event of a bioterrorist attack, local community organizations need to know how to respond in order to avoid and contain mass public panic. These "first responder" organizations include local law enforcement, the fire department, state and local governments, hospitals, HAZMAT teams, emergency medical services, and area public health departments (Crosse 2003). The involvement of and communication among these organizations will be vital to controlling an infectious disease outbreak and to calming the mass public panic that will ensue (Powner 2003).

The emergency room is not the only health provider that will be flooded with victims of bioterrorist attacks. Physician involvement in planning for bioterrorism attacks is severely lacking (Kahn 2003). Primary care physicians will also receive an influx of patients in the event of a bioterrorist attack and have a critical role in any public health emergency (Lane and Fauci 2001). A survey done in 2002 of 1,000 AMA physicians showed only 21% of physicians felt prepared to handle a bioterrorist attack, and only 22% felt hospitals in their practice areas were prepared (Alexander and Wynia 2003). Also, these physicians will be either admitting patients to hospitals or referring patients to hospitals, which are other reasons why planning efforts need to be coordinated with local physicians. The American College of Public Medicine estimates that $22.2 million is needed to adequately train physicians to deal with a mass biological agent attack (Kahn 2003).

Educating Hospital Staff

In June 2002 the Public Health Security and Bioterrorism Preparedness and Response Act was passed, which, among other things, was aimed at improving education for health care professionals (Frist 2002). This bill highlights the need for hospital staff to be able to treat these biological agents, many of which have never been seen by this generation of health care workers. Victims of bioterrorism events are going to go to hospital emergency rooms. Emergency room and infectious disease staff need to be better educated and trained to recognize the signs and symptoms related to biological agents. Several of these biological agents also result in physical signs and symptoms similar to other common illnesses. Anthrax and plague, for example, exhibit *(Continued, Page 13)*

Bioterrorism Preparedness *(Cont. from Page 12)* signs similar to influenza. Smallpox is also highly communicable, so emergency rooms staff needs to know how and where to isolate possible victims (Powner 2003).

Some of the specific precautions hospital staff need to be alerted to vary depending on how the biological agent is released and what type of agent is released, as shown in Table 1. Standard precautions include washing hands, wearing gloves and masks, and sterilizing equipment. These are all precautions currently taking place in hospitals. Contact precautions include the isolation of patients and equipment likely to be infected, as well as frequent cleaning of equipment (Werner 2002). Droplet precautions require masks to be worn at all times, patient isolation, and maintaining as much distance as possible between health care providers and patients (Werner 2002). Airborne precautions require patients to be put in isolated areas "with negative pressure, a minimum of six air changes per hour, and appropriate filtration of air before discharged" (Werner 2002).

Hospitals also need to look at vaccinating their essential first responder staff against infectious diseases as well. While the benefits of the anthrax vaccine remain questionable, the smallpox vaccine does pose less of a threat. The CDC Advisory Committee on Immunizations Practice (ACIP) released a statement in June 2003 recommending the formation of "smallpox response teams" to receive small pox vaccinations (DHHS 2003). These 40 person teams include emergency room nurses and physicians, epidemiologists, ICU and PICU staff, infectious disease consultants, respiratory therapists, radiology technicians, engineers, and selected security and facilities management staff (DHHS 2003).

Table 1. Bioterrorism Infection Control Precautions

All Bioterrorism	Standard Precautions
Smallpox	Standard, Contact, and Airborne
Viral hemorrhagic fever (VHF)	Standard, Contact, and Airborne
Brucellosis	Standard and Contact
Anthrax	Standard and Possibly Airborne
Pneumonic plague	Standard and Droplet

Source: Healthcare Purchasing News, December 2002

Improving Information Technology and Disease Surveillance

Information technology (IT) is vital to improving communication and the sharing of information in the event of a bioterrorism attack. In November 2002, the Agency for Healthcare Research and Quality (AHRQ) released a report with suggestions for IT improvements. IT can be used in a variety of ways to help contain the effects of a bioterrorist attack. It can be used to gain information from public health departments, which can help to isolate the cases of disease related to a bioterrorist attack from those that may have naturally occurred (Powner 2003).

Information technology can also be used to send information to public health departments for record keeping purposes and surveillance. The CDC is using IT for syndromic surveillance which tracks the number of people visiting emergency rooms with symptoms similar to those presented with certain biological agents (McCarthy 2001). Some of these symptoms are fever, headache, and cough. A rise in the number of patients with these symptoms would cause the CDC to put up a "red flag." IT is also being used to monitor the number of over-the-counter drugs being purchased, such as Tylenol, which victims of an attack would be likely to purchase to treat initial symptoms (McCarthy 2001). Bioterrorism preparedness does not stop at the emergency room either. The Association of Public Health Laboratories has developed an online education program for clinical laboratories. This program should accompany training already occurring in labs *(Continued, Page 14)*

Bioterrorism Preparedness *(Cont. from Page 13)* for surveillance of bioterrorist agents (Business Wire 2003). The program highlights the detection of anthrax, tularemia, plague, and brucellosis, which is a Category B infectious agent according to the CDC. The DHHS has also designed a new computer program to aid hospitals in dispensing vaccines and antibiotics in the event of a bioterrorist attack (U.S. Newswire 2003).

Additional Equipment and Staff

To successfully treat the victims of a bioterrorist attack requires large quantities of specialized equipment and medications. Some of the equipment needed by hospitals includes personal protective equipment, mass decontamination shower units, and ventilators, as well as isolation/ quarantine beds and supplies of antibiotics, antidotes, and vaccines. Purchasing all of this equipment is one solution, but another way hospitals can acquire the equipment needed for bioterrorism preparedness is through the sharing of resources with other area hospitals. A study involving 1,482 urban hospitals reported that half currently have resource sharing measures already in place (Crosse 2003).

Resource sharing is also not limited to equipment. Many hospitals also have staff sharing agreements in place in the event of a bioterrorist attack. Hospitals can test how well they have planned for the incorporation of community organizations during their JCAHO required drills. The Joint Commission requires hospitals to complete four drills annually to deal with the outbreak of infectious diseases, which include biological agents.

Evaluation of Bioterrorism Preparedness Measures

With few guidelines currently available for bioterrorism preparedness, hospitals are on their own for planning new policies and implementing new procedures. Hospitals must perform an evaluation of their capacity to address both the direct and indirect effects of a bioterrorism event. Table 2 suggests an approach for hospitals to use to evaluate the action steps discussed above. Hospitals located in areas where the threat of an attack is low (e.g., small urban areas, towns and rural communities) should focus on different measures than hospitals in high threat areas (e.g., metropolitan and large urban areas, and smaller communities having vulnerable military and industry sites).

Hospitals in low threat areas should focus preparedness efforts on staff training and community involvement. By training staff and developing policies with surrounding communities, low threat area hospitals can be called upon for necessary support by hospitals in high threat areas. Hospitals in high threat areas should focus their bioterrorism preparedness measures more on information technology, disease surveillance, and equipment. If an attack occurred, information technology and disease surveillance will help to alert hospitals more quickly and allow them to begin appropriate treatment. Additional equipment to treat bioterrorism victims will also be needed in the event of a direct attack in a high threat area.

Table 2. Evaluation of Bioterrorism Preparedness Measures

Type of Bioterrorism Preparation	Cost to Hospital	Benefit to Hospital
Community Involvement	Low	Medium
Educating Hospital Staff	Medium	High
Improving IT and Disease Surveillance	High	High
Additional Equipment and Staff	High	Medium

Source: Compiled from author's review of relevant literature.

Funding Bioterrorism Preparedness Measures

As the current literature suggests, many hospitals are currently *(Continued, Page 15)*

Bioterrorism Preparedness *(Cont. from Page 14)* ill equipped to successfully handle a bioterrorist attack. A March 2003 statement from the Joint Commission described bioterrorism preparedness as "a brewing cataclysm of underfunding, inexperience and under-preparedness of emergency response capabilities across America's communities" (PR Newswire 2003). Much of this "under-preparedness" is due to a lack of funding. Bioterrorism preparedness is expensive and most hospitals have trouble investing funds into resources that they may never utilize (Crosse 2003). The federal government has dispersed money in large amounts to deal with bioterrorist attacks, but little of this money has been specifically directed toward hospitals. Money is being given to government agencies and local and state government, but hospitals are finding themselves waiting for the funds to trickle down to them. The financial burden of preparing for bioterrorism has fallen on state and local governments and the federal government needs to continue financial support if they intend to mount a serious defense to bioterrorism. The Department of Health and Human Services (DHHS), along with the CDC, NIH, FDA, EPA, DOE, and the Department of Homeland Security are working together to help better prepare the public for bioterrorism attacks, but efforts have yet to entirely meet the needs of hospitals (Business Wire 2003).

In the wake of the anthrax scares of 2001, $1 billion was distributed to the states for improving information technology (Trembly 2002). In 2002, $125 million was allocated through DHHS's Health Resources and Services Administration (HRSA) to increase hospitals abilities to deal with a bioterrorist attack, however it did require organizations to apply for the funding (Greene 2002). To apply for the funding hospitals had to first conduct a needs assessment for bioterrorism preparedness policies. After initial approval, hospitals then had to submit a second, more detailed plan of implementation addressing the issues of "medications and vaccines; personal protection, quarantine, and decontamination; communications; and biological disaster drills" (Crosse 2003). This initial $125 million from HRSA only works out to $21,000 per hospital, a mere drop in the bucket compared to what hospitals need. The American Hospital Association estimates $1.9 million is needed for each of the 5,800 American hospitals, for a total of $11 billion (Greene 2002).

In March 2003, HRSA again allocated another $498 million to the states, this time through its National Bioterrorism Hospital Preparedness Program. In 2003, President Bush also allocated an additional $300 million to the CDC to increase supplies in the Strategic National Stockpile. The Strategic National Stockpile is a federal government supply of pharmaceuticals, antidotes, and equipment that can be delivered to bioterrorism attack sites (Crosse 2003). Bioterrorist attacks are a threat to national security and should be funded as such. With limited financial resources available to adequately prepare themselves, hospitals should consider preparing regionally rather than individually (Greene 2002).

By sharing resources and planning bioterrorism policies regionally, hospitals focus on preparing an entire region, rather than just individual hospitals. Texas has taken a regional approach in preparing for bioterrorism. Using the money from HRSA, they have developed a bioterrorism guidance manual to assist Texas hospitals and have made their bioterrorism preparedness a regional effort. There are also plans to develop similar manuals to address planning for other types of terrorist attacks (PR Newswire 2003). Texas is also already working with South Dakota to develop their own measures, similar to Texas' (PR Newswire 2003).

Conclusion

It should not have to take a specific event actually occurring on American soil to motivate hospitals to elevate their bioterrorism preparedness. Bioterrorism preparedness needs to be one of the top issues on hospital agendas, especially with the ongoing world conflicts and the proliferation of weapons of mass destruction. Hospitals must continue to do the best they can with what funding they have received to prepare their facilities and to protect their patients and the larger *(Continued, Page 16)*

Bioterrorism Preparedness *(Cont. from Page 15)* community. By focusing on improving community involvement and information technology, as well as obtaining access to additional equipment and training staff, hospitals can elevate their preparedness for bioterrorism. Hospitals have been the center of care in communities for centuries, and will continue to be the primary source of care for the victims of bioterrorism and other events in the post-9-11 era.

References

Alexander, C. and Wynia, M. 2003. "Ready and Willing? Physicians' Sense of Preparedness for Bioterrorism." *Health Affairs*. 22(5): (189-197).

Barbera, J. and Macintyre, A. 2002. "The Reality of Modern Bioterrorism Response." *The Lancet*. 360 (9350): 33-34.

Bartlett, J. 2001. "Mobilizing Professional Communities." *Public Health Reports.* 116 (6): 40-44.

Business Wire. 2003. "Online Bioterrorism Training Course to Train Clinical Laboratories How to Respond to Public Health Threat." *Business Wire, Inc*. 23 June 2003.

Crosse, M. 2003. "Most Urban Hospitals Have Emergency Plans but Lack Certain Capacities for Bioterrorism Response." *General Accounting Office*. GAO-03-924.

Frist, B. 2002. "Public Health and National Security: The Critical Role of Increased Federal Support." *Health Affairs*. 21(6): 117-130.

Greene, J. 2002. "Readying bioterrorism defenses: Preparations continue despite inadequate finds." *Materials Management in Health Care*. 11 (5): 32-34.

Kahn, L. 2003. "A Prescription for Change: The Need for Qualified Physician Leadership in Public Health." *Health Affairs*. 22 (4): 241.

Lane, H. and Fauci, A. 2001. "Bioterrorism on the Home Front: A New Challenge for American Medicine." *Journal of the American Medical Association*. 286(20): 2595-2597.

McCarthy, M. 2001. "Attacks heighten U.S. concern about threat of bioterrorism." *The Lancet*. 358 (9287): 1071.

Powner, D. 2003. "Information Technology Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies." *General Accounting Office.* GAO-03-139.

PR Newswire. "Texas Takes a Leading Role in Regional Hospital Bioterrorism Planning." *PR Newswire Association, Inc.* Financial News 8 April 2003.

Tieman, J. 2002. "Hospitals create new models as they gird for bioterrorism." *Modern Healthcare*. 32 (35): 8.

Treat K., Williams J., Furbee P., et al. 2001. "Hospital preparedness for weapons of mass destruction incidents: An initial assessment" *Annals of Emergency Medicine* 38 (5):562-565.

Trembly, A. 2002. "Current Technology is Inadequate for Bioterrorism Response." *National Underwriter*. Life & Health/Financial Services Edition. 4 November 2002.

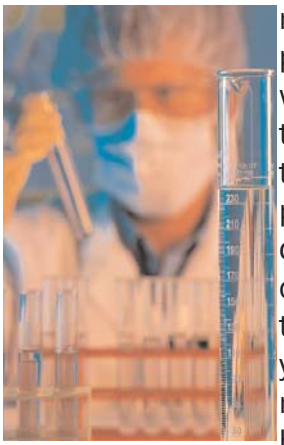
U.S. Department of Health and Human Services. 2003. "Advisory Committee on Immunization Practices (ACIP) Statement on Smallpox Preparedness and Vaccination." *Centers for Disease Control and Prevention*. 18 June 2003.

U.S. Newswire. 2003. "New Model Helps Hospitals and Health Systems Better Respond to Potential Bioterrorism." *U.S. Newswire, Inc*. 26 June 2003.

Werner, C. 2002. "Hospitals must be ready for bioterrorism." *Healthcare Purchasing News*. December 2002: 30. ❖

Call to Action *(Cont. from Page 3)*
technologies in healthcare diagnostics and treatments in the U.S. enables the sector to be more efficient, but it may also increase the industry's overall vulnerability to cyber attack. Companies will continue to develop less invasive technologies, making treatment more accessible to both ends of the patient spectrum, young and old[1]. Information technology will continue to drive advances with implications on both clinical and supporting technologies utilized for the delivery of healthcare services. For instance, by year-end 2003, PDA-sized mobile devices for content look-up, drug-drug interaction checking, and dosage calculations will be used by more than one-third of U.S. physicians. That number is expected to grow to represent at least half of U.S. physicians by the end of 2004[3].

At the same time, the healthcare infrastructure as a whole faces a



multitude of problems with respect to providing the highest possible quality of care. Over the past 50 years, the majority of healthcare facilities have become obsolete, both the physical plant and technology[1].

Obsolete healthcare facilities often result in lower levels of quality of care and, simultaneously, an increased number of risks associated with patient safety. Additionally, increasing demands for higher levels of care place additional strains on organizations to invest more readily in their physical and technology infrastructures. Responding to capacity issues therefore requires the redevelopment of existing facilities, which is becoming increasingly more expensive per square foot. Between creating new capacity and replacing existing capacity, the industry may have to spend more than a half-trillion dollars on healthcare facility construction over the next 20 years[1]. For example, the Centers for Medicare & Medicaid recently predicted that U.S. spending on hospital and nursing home construction would grow from $21.3 billion in 2002 to $33.1 billion in 2010[4].

With the release of the recent Institute of Medicine companion studies, "To Err is Human" and "Crossing the Quality Chasm," it is clear that the healthcare industry will require major IT investments to enable major advancements in patient safety and a higher quality of patient care. A requisite transformation from paper-based to electronic medical records (EMR) is underway in the provider sector. EMR will be coupled with automated decision support tools that will link new scientific knowledge with patient conditions and provide appropriate rules and alerts to guide the adoption of best clinical practices, reduce variation in care, and drive significant improvements in patient outcomes. Leapfrog Group reports that, based on a Computerized Provider Order Entry (CPOE) standard study that included 948 urban and suburban hospitals, 5 percent have "fully implemented CPOE" and 25 percent expect to have CPOE in place by 2004[5]. The interconnectedness of healthcare systems is increasing at an alarming rate, as is the use of wireless access.

Additionally, patients are becoming more and more responsible for the care they receive. In 2000, almost 61 percent of healthcare seekers (45 million Americans) noted that the Internet improved the way they managed their health[2].

The healthcare infrastructure is therefore changing dramatically, giving rise to a growing array of threats and vulnerabilities as the industry becomes more dependent on the support of cyber and physical infrastructure to deliver patient care.

In light of the challenges that face the current healthcare infrastructure, the ability to provide high levels of quality care depends on the healthcare workforce. Currently the national vacancy rates for 2001 indicate that there are significant shortages of medical professionals: nurses (11 percent), pharmacists (21 percent), radiology technicians (18 percent), and lab technicians (12 percent)[6]. Given the demand for growth, the industry will need more clinicians of all

(Continued, Page 18)

Call to Action *(Cont. from Page 17)* types, as well as effective managers, to deliver the care that is needed in this country over the next 20 years[1].

Financing:

The healthcare financing system consists of both government and private providers. Medicare and Medicaid are government-funded programs that provide healthcare for patients over 65, or the disabled and low-income individuals respectively. Private insurance companies provide coverage to patients primarily through their employers. Currently the healthcare financing system does not account for 39 million Americans[7]. The burden of the uninsured on the healthcare system is great. The amount of uncompensated care delivered by non-federal community hospitals grew from $6.1 billion in 1983 to $20.7 billion in 19998. Over the next several years, increasing demand, political processes, and growing consumer dissatisfaction will be key drivers of healthcare coverage. There is little dispute that the demand for services and funding will increase primarily as a result of new technology, a growing aging population, and disease. In addition, consumer dissatisfaction will persist and could increase in areas related to employer and government coverage, access and quality barriers, and the uninsured.

These components are key factors in shaping the current and future states of healthcare. As healthcare becomes more interconnected and dependent on technology to support delivery of patient care and as patients increasingly access the Internet for health information, the threats and vulnerabilities facing healthcare's cyber security also increase. The healthcare sector must recognize that the growing vulnerabilities facing our industry are real. The sector must now take the appropriate actions to address the increasing number of threats and ways of responding to them.

1 Wietecha, M., Cosovich, CJ., DeChant, T., Nussbaum, G., & Wimpey, A. (2002). Special Article: A View of the U.S. Health Care System and Implications for Providers Year 2020. Kurt Salmon Associates, 1-16.

2 Fox, S & Rainie, L. *"Vital Decisions: How Internet users decide what information to trust when they or their loved ones are sick."* 2002. http://www.pewinternet.org/reports/ (23 January 2003).

3 Rishel, W., Hieb, B., & Klein, K. (2002). Predictions for Underlying Technologies in Healthcare. Gartner Research. 1-6.

4 Center for Medicare and Medicaid Centers, 2002. http://cms.hhs.gov

5 Leapfrog Group, 2000. http://www.leapfroggroup.org/

6 Health Care Advisory Board. (2001). Competing for Talent: Recovering America's Hospital Workforce. The Advisory Board Company.

7 U.S. Census Bureau, Department of Commerce, Economic and Statistics Administration, *"Health Insurance Coverage: 2001"* 2001. http://www.census.gov

8 American Hospital Association, 2002. http://www.aha.org ❖

The CIP Project is part of the National Center for Technology and Law at the George Mason University School of Law. It is a joint initiative between GMU and JMU that examines law, technology, and policy to find comprehensive solutions to the most pressing CIP issues for policy makers and critical infrastructure owners and operators. The CIP Project was launched in May 2002. The CIP Project encourages participation by representatives from all levels of government, academia, and private industry.

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Project. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for The CIP Report, please click on this link: http://listserv.gmu.edu/archives/cipp-report-l.html.